Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Estadística

Imagen de las principales marcas de la industria de TI sobre seguridad informática en las organizaciones del Perú

TESIS

Para optar el Título Profesional de Licenciado en Estadística

AUTOR

Jorge Alejandro MALCA RODRÍGUEZ

ASESOR

Mg. María Estela PONCE ARUNERI

Lima, Perú

2019

Referencia bibliográfica

Malca, J. (2019). *Imagen de las principales marcas de la industria de TI sobre seguridad informática en las organizaciones del Perú*. Tesis para optar el título profesional de Licenciado en Estadística. Escuela Profesional de Estadística, Facultad de Ciencias Matemáticas, Universidad Nacional Mayor de San Marcos, Lima, Perú.

HOJA DE METADATOS COMPLEMENTARIOS

CODIGO ORCID DEL AUTOR: No tiene

CODIGO ORCID DEL ASESOR: 0000-0002-3091-5741

DNI: 10307159

GRUPO DE INVESTIGACIÓN: Trabajo individual

INSTITUCIÓN QUE FINANCIA PARCIAL O TOTALMENTE LA INVESTIGACIÓN: Ninguna

UBICACIÓN GEOGRÁFICA DONDE SE DESARROLLÓ LA INVESTIGACIÓN. DEBE INCLUIR LOCALIDADES Y COORDENADAS GEOGRÁFICAS:

Lima – Miraflores

12° 7′ 3″ S, 77° 2′ 35″ W

-12.1175°, -77.043056°

AÑO O RANGO DE AÑOS QUE LA INVESTIGACIÒN ABARCÓ:

Marzo 2017 – Abril 2007

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Fundada en 1551
FACULTAD DE CIENCIAS MATEMATICAS
Ciudad Universitaria – Pabellón de Matemáticas
Teléfonos: 452-0805 – 464-6442 Telefax: 4515815– Casilla Postal: 05 – 0021
Av. Venezuela s/n – Lima – Perú

PROGRAMA DE TITULACION PROFESIONAL 2006

Escuela Académico Profesional de Estadística

ACTA DE SUSTENTACION DE MONOGRAFIA PARA OBTENER EL TITULO PROFESIONAL DE LICENCIADO EN ESTADISTICA

En la Ciudad Universitaria, Facultad de Ciencias Matemáticas, siendo las 5:00 horas del día 29 de Enero del año 2007, se reunieron los docentes designados como miembros del Jurado de Monografía:

- Lic. Montes Quintana Grabiela — Presidenta
- Mg. Ponce Aruneri María Estela — Asesora

Para la sustentación de la monografía intitulada: **"IMAGEN DE LAS PRINCIPALES MARCAS DE LA INDUSTRIA DE TI SOBRE SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES DEL PERÚ"**, presentada por el participante Bachiller **Malca Rodríguez, Jorge Alejandro,** para obtener el Título Profesional de Licenciado en Estadística.

Luego de la exposición de la monografía, el Presidente invitó al expositor a dar respuesta a las preguntas formuladas.

Hecha la evaluación correspondiente por los miembros del jurado, el expositor mereció la aprobación. Sobresaliente obteniendo como calificativo promedio la nota de Dieciocho (18) (letras y números).

A continuación los miembros del Jurado, dan manifiesto que el participante Bachiller **Malca Rodríguez, Jorge Alejandro**, en virtud de haber aprobado la sustentación de su monografía, será propuesto para que se le otorgue el Título Profesional de Licenciado en Estadística.

Siendo las 6:00 p.m. horas, se levantó la sesión, firmando para constancia la presente acta en tres (3) copias originales.

Mg. Ponce Aruneri María Estela
(Asesora)

Lic. Montes Quintana Grabiela
(Presidenta)

FICHA CATALOGRÁFICA

MALCA RODRÍGUEZ, JORGE ALEJANDRO

Imagen de las principales marcas de la industria de tecnologías de la información sobre Seguridad Informática en las Organizaciones del Perú, (Lima) 2007.
Xii, 118 p. (UNMSM. Licenciado en Estadística, 2007)
Monografía, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas. E.A.P de Estadística.
UNMSM/ FdeCM.

Agradezco a Dios que siempre me ilumina, a mi esposa Miriam y mi hijo Diego, a mis padres Ernesto y Rosa quienes me apoyaron anímica y económicamente. A la valiosa asesoría de la Mg. María Estela Ponce Aruneri quien me apoyo en los temas multivariados aplicados en este trabajo y a mis amigos que siempre ejercieron una presión muy agradable,

“Nunca es tarde para alcanzar tus metas”

RESUMEN

IMAGEN DE LAS PRINCIPALES MARCAS DE LA INDUSTRIA DE TECNOLOGIAS DE LA INFORMACION SOBRE SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES DEL PERÚ

JORGE MALCA RODRIGUEZ

NOVIEMBRE 2019

Orientador: Mg. María Estela Ponce Aruneri.

Título: Licenciado en Estadística.

La presente investigación tiene como objetivos: descubrir el estado en que se encuentra la seguridad informática, lógica y física de las organizaciones privadas y públicas consumidoras de la industria de Tecnología de Información en el Perú en el año 2007; caracterizar a las organizaciones consumidoras del mercado de Tecnología de Información, respecto al tema de seguridad informática; y el posicionamiento de las principales marcas.

Existen 9208 organizaciones (segmentadas según su facturación ultima anual como Corporativas/Grandes/Medianas/Gobierno); el estudio se basó en una muestra aleatoria simple de cada uno de estos tipos de organizaciones (segmentación). Se utilizaron métodos descriptivos univariantes y multivariantes (análisis factorial de correspondencias múltiples) para analizar los datos, lo que permitió conocer el mercado de Tecnología de Información, su evolución y participación de las marcas competidoras en dicho mercado y; por el lado de los consumidores, se pudo caracterizar a las organizaciones en función al nivel de la seguridad informática existente en cada una de ellas.

Se muestra que las organizaciones corporativas y grandes valoran más la seguridad lógica, las empresas medianas y organizaciones de gobierno por el contrario se caracterizan por ofrecer más importancia al tema de seguridad física.

Cisco es la marca, en términos generales, considerada como la más segura según la opinión de los encuestados

PALABRAS CLAVE: IMAGEN, MARCAS, SEGURIDAD INFORMÀTICA,

SUMMARY

IMAGE OF THE MAJOR BRANDS OF THE TECHNOLOGY INDUSTRY OF INFORMATION ON COMPUTER SECURITY IN THE ORGANIZATIONS OF PERU

JORGE MALCA RODRIGUEZ

SEPTEMBER 2019

ADVISER: MG. MARIA ESTELA PONCE ARUNERI.

TITTLE TO BE OBTAINED LICENCIADO EN ESTADISTICA

The purpose of this research is to: discover the state of computer, logical and physical security of private and public consumer organizations of the Information Technology industry in Peru in 2007; characterize the consumer organizations of the Information Technology market, regarding the issue of computer security; and the positioning of the main brands.

There are 9208 organizations (segmented according to their latest annual turnover as Corporate / Large / Medium / Government); the study was based on a simple random sample of each of these types of organizations.

There are 9208 organizations (segmented according to their last annual turnover as Corporate / Large / Medium / Government); The study was based on a simple random sample of each of these types of organizations (segmentation). Univariate and multivariate descriptive methods (multiple correspondence factor analysis) were used to analyze the data, which allowed to know the Information Technology market, its evolution and participation of competing brands in said market and; On the consumer side, organizations could be characterized according to the level of information security in each of them.

It is shown that large and corporate organizations value logical security more, medium-sized companies and government organizations on the contrary are characterized by offering more importance to the issue of physical security.

Cisco is the brand, in general terms, considered the safest in the opinion of respondents.

Key words: Image - -Brands - -Informatic Security - Multiple Correspondences.

INDICE

CAPITULO I:
ASPECTOS GENERALES

1.1 Planteamiento del problema

Es conocido que la seguridad tanto informática como física en las organizaciones afecta claramente al quehacer de las organizaciones, sus planes estratégicos y como no mencionar el personal. En tal sentido es necesario conocer el estado actual de la seguridad física y lógica en las organizaciones para poder concientizar a los responsables de la seguridad en las organizaciones y para poder cooperar en la dinámica del mercado de TI ya que mientras más información se genere, muchas estrategias de las marcas competidoras en el mercado se redirigirán o afinaran favoreciendo tanto a la economía de las marcas como al usuario.

1.2 Objetivo General

Caracterizar las organizaciones del Perú en función a sus características de seguridad informática y física.

1.3 Objetivos Específicos

Determinar la situación de la seguridad lógica y física de las organizaciones.

Analizar la vulnerabilidad en la seguridad informática de las organizaciones del Perú.

Conocer la participación en el mercado de TI de las diferentes marcas tales como, UPS, antivirus, antitroyanos, firewalls, adware, spyware entre otros.

Conocer el porcentaje de organizaciones que tienen algún servicio de seguridad en modalidad de Outsourcing.

1.4 Justificación

El presente estudio se realiza cada tres años por una empresa de consultoría privada con el fin de conocer la evolución de las medidas tomadas en cuanto el tema estudiado.

El motivo es analizar las vulnerabilidades, analizar también las políticas de seguridad adoptadas y medición de la importancia que le otorgan los principales directivos de las organizaciones al tema de seguridad.

Es para mí una satisfacción poder aplicar determinados conocimientos adquiridos a lo largo de mis estudios universitarios.

Personalmente, este trabajo de investigación es un catalizador del empeño que realizo por actualizarme en el desarrollo y aplicación de diferentes técnicas para poder superarme profesionalmente y aumentar mi valor como analista de este mercado.

CAPTULO II:
MARCO TEÓRICO

2.1 Conceptos Generales

Se utilizó en gran medida estadística descriptiva para conocer el posicionamiento, participación de mercado de las diferentes marcas de la industria de TI.

Se calcularon porcentajes para obtener la participación de mercado y penetraciones

La diferencia entre participación y penetración radica en la modalidad de respuesta; mientras que para la participación de mercado calculada los porcentajes (participaciones de mercado) suman 100%, la penetración no suma necesariamente 100% ya que trabaja con respuestas múltiples.

El presente trabajo de investigación se basó también sobre el conocimiento del mercado de cómputo de los analistas expertos que lo integran.

2.2 Análisis de Correspondencias

Es una técnica estadística descriptiva que permite la reducción de dimensión del tema en estudio y que gráficamente se puede analizar mediante la elaboración de mapas perceptuales. Estos mapas representan gráficamente la/s relación/es que existen entre individuos y sus características en estudio.

La medida de asociación empleada por esta técnica se basa en la chi-cuadrado la cual permite conocer la relación entre categorías de las variables nominales en estudio. La técnica “reduce” la dimensión basado en la proximidad entre los individuos en estudio. Esta proximidad “matemática” permite indicar el nivel de asociación.

En términos generales, el AFC persigue dos objetivos:

El primer objetivo busca identificar la asociación entre las categorías de una fila o una columna y estudiar la posibilidad de combinar las modalidades de estas.

El segundo objetivo busca identificar la asociación entre todas las categorías de las filas y columnas.

2.2.1 Análisis de Correspondencias Simple

Esta técnica estadística tiene como objetivo identificar la/s relación/es existente/s entre dos variables nominales obtenidas de una tabla de contingencias plasmada en un espacio de unas cuantas dimensiones descubriendo paralelamente las relaciones que existen entre las categorías de cada una de las variables en estudio. las distancias sobre este espacio determinadas por los puntos de cada categoría de cada variable reflejan la relación que existe entre ellas.

Esta técnica contempla también, en el análisis de las tablas de contingencia, el estudio de los perfiles fila y columna y también el estudio y evaluación de la independencia de esta utilizando el estadístico chi cuadrado.

Es esperado que este estudio de los perfiles pueda ser muy complejo por la gran cantidad de perfiles existan y por consiguiente no se podrá conocer estructuralmente la dependencia entre ellas.

Este análisis de tablas de contingencias a menudo no puede representar mediante gráficos las relaciones entre las variables en estudio.

2.2.2 Análisis de Correspondencias Múltiples

En general, el análisis multivariado permite resumir grandes cantidades de información por medio de relativamente pocas dimensiones.

La técnica de análisis factorial de correspondencias múltiples permite visualizar un tema o problema investigado, el cual se mide en función de varios factores, en una dimensión reducida y que sin embrago no “pierde” la información de las variables estudiadas, sino que recoge y opera tomando información de todas las variables en conjunto.

Esta técnica en especial trabaja con varias variables categóricas I, J, K, etc. Y estudia las relaciones entre cualquier número de estas variables y tomando en cuenta también las diferentes modalidades de respuesta que tenga cada variable.

No ahondaremos mucho en cómo opera esta técnica, más bien daremos una visión general de que es lo que realiza.

Trabaja con tablas disyuntivas completas y es sobre esta tabla que se basa para operar.

A manera de una fácil comprensión, esta técnica permite visualizar en un mismo espacio el comportamiento de los individuos estudiados (en nuestro caso las organizaciones) y las variables categóricas. Es esta la razón de ser de esta técnica ya que, de ésta, manera podemos "visualizar" en un mismo plano el tema tratado.

En conclusión, esta técnica me permitió caracterizar a las organizaciones en función a las variables estudiadas.

El Análisis Factorial de Correspondencia Múltiple (AFCM) es simplemente la generalización del AFCS. La técnica estadística que permite visualizar a más de dos variables de tipo cualitativo en un gráfico y que además permite evidenciar la relación entre ellas es el AFCM. De igual manera como el AFCS se dedica a estudiar la relación de dos variables de tipo cualitativo I y J observadas en la misma población (en una tabla de contingencia), el AFCM se dedica a estudiar las relaciones de un numero de características indeterminado considerando todas las modalidades de estas.

Tabla disyuntiva

Un AFCM está diseñado para tablas disyuntivas completas.

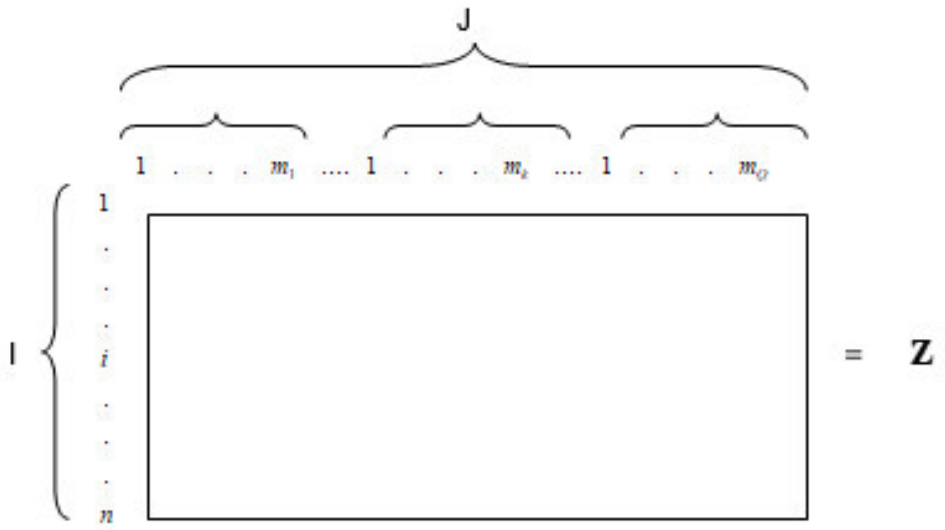
Una tabla disyuntiva completa Z queda definida mediante:

Un conjunto de individuos i=1,2,..., n.

Un conjunto de variables o preguntas J1, J2,...., Jk,…,Jq

Un conjunto de modalidades para cada pregunta 1,...., mk.

El número total de modalidades es $J = \sum_k m_k$



Z es la matriz expandida binaria, tabla disyuntiva I x J, el elemento Zij puede tomar el valor 1 o 0 según que el individuo i haya elegido la modalidad j o no.

Luego B = Z'Z es la matriz de Burt.
El análisis de correspondencia implica la descomposición de la Tabla de Burt en sus autovalores y autovectores. La obtención, selección e interpretación de los factores es similar al AFCS.

Análisis de la tabla Z

La manera en el AFCS puede analizar esta matriz Z la cual es una tabla disyuntiva completa es considerándola como una yuxtaposición de tablas de contingencia. El resultado de este análisis es la representación de todas las modalidades o columnas y los individuos de manera simultánea.
A continuación, podemos apreciar las particularidades de un AFCS aplicado a una tabla disyuntiva completa.

Significado de la terminología
Los elementos de Z, zij = nij son 1 o 0.

$n_{i.} = \sum_i n_{ij} = Q$, el número de preguntas

$\frac{f_{ij}}{f_{i.}} = \frac{n_{ij}}{n_{i.}} = \frac{1}{Q}$, el número de preguntas 1 o 0 según el individuo haya elegido o no la modalidad j.

Diagonalización de la matriz Inercia

Para obtener los factores es necesario diagonalizar la matriz V que está definida por: $V = \frac{1}{Q} D^{-1} B$

Donde la matriz $B = Z'Z$, es la tabla de Burt. Es una matriz simétrica formada por Q2 bloques. Los bloques de la diagonal son las tablas diagonales que cruzan una pregunta con ella misma $Z_k^{'} Z_{k'}$. Sus elementos son las frecuencias de asociación de las modalidades correspondientes.

	J_1	J_2	...	J_Q
J_1	0 / 0	C_{12}		C_{1Q}
J_2	C_{21}	0 / 0		C_{2Q}
. . .				
J_Q	C_{Q1}			0 / 0

La matriz D es una matriz diagonal cuyos elementos diagonales son los de la matriz de Burt, los efectivos de cada modalidad. El resto de cada modalidad. El resto de los elementos son nulos.

Será necesario entonces a diagonalizar: V=(1/Q)D-1B. Resultado de esta diagonalización se obtienen los autovalores y autovectores que ofrecen una solución óptima a V.

Del Análisis factorial de correspondencias simple tenemos las relaciones de transición: $F\alpha(i) = \sqrt{1/\lambda\alpha \sum (f_{ij}/f_i)\, G\alpha(j)}$ y $G\alpha(j) = \sqrt{1/\lambda\alpha \sum (f_{ij}/f_i)\, F\alpha(i)}$. Donde λα es el valor propio asociado al factor α.

Esto significa (en AFCS) que la proyección del punto i sobre el eje α Fα(i) es el baricentro de las proyecciones j sobre el mismo eje. De la misma manera, la proyección del punto j sobre el eje α, G α(j), es el baricentro de las proyecciones de los puntos i sobre el mismo eje. Son estas relaciones las que permiten transitar de un espacio a otro y representar simultáneamente sobre el mismo plano los puntos fila y columna.

Ahora, aplicado a nuestro caso (AFCM), las fórmulas equivalentes serian:

Fα(i) = (1/λα (1/Q)∑KijG(j) y Fα(i) = (1/λα (1/Q)∑KijG(j).

Kij=1 si el individuo i posee la modalidad j y cero cuando no la posee. La proyección del punto i (individuo i) sobre el eje α, Fα(i) es el baricentro de las proyecciones de los puntos modalidades sobre el mismo eje. (1/Q) es el peso que afecta a cada uno de estos puntos proyectados, donde Q es el número de variables categóricas.

Asimismo, la proyección de un punto j (modalidad) sobre el eje α, Gα(j), es el baricentro de la proyección de los individuos que poseen esa modalidad.

Centros de gravedad en las nubes y subnuves

El centro de gravedad de la nube de puntos variables N(J) en AFCS es $\sqrt{f_{i.}}$.

En este caso es la distribución uniforme $1/\sqrt{n}$. En consecuencia

$n_{i.} = Q, \sum_i n_{i.} = nQ$, luego $f_{i.} = 1/n$ y $\sqrt{f_{i.}} = 1/\sqrt{n}$

El centro de gravedad de las modalidades de cada pregunta, cada una ponderada por su peso, es el mismo que el de la nube de modalidades N(J), $1/\sqrt{n}$.

En efecto, el centro de gravedad de la subtabla I x Jk se obtiene a partir de su distribución marginal. Como sólo recoge una pregunta, la suma de cada fila es 1 y el total de la tabla n, de donde $f_{i.} = 1/n$ y en consecuencia el centro de gravedad de las modalidades de esa pregunta es $1/\sqrt{n}$.

Como el AFC es centrado y el centro de gravedad de las modalidades de una pregunta coincide con el del conjunto J, y con el origen, las

modalidades de cada cuestión están centradas en torno al origen, no pudiendo tener todo el mismo signo.

Cálculo de estadísticos de control

Como en cualquier análisis factorial, se calculan las ayudas a la interpretación para cada fila (individuo) y columna (modalidad).

Contribuciones absolutas (Ctaα(I))

Representan la proporción de la varianza que es explicada por un eje debido a un perfil (i,j). Esto significa que, estas contribuciones nos permiten conocer a las variables responsables de la contribución de un factor. Mide cuanto aporta el punto (i,j) en la inercia (variabilidad) de la proyección de un factor. Muestra también, porcentualmente, que tan importante es cada categoría en la definición de cada uno de los ejes. Geométricamente representa el porcentaje de inercia de cada eje, que está definido por cada modalidad de la variable. En decir expresa la participación que tienen el elemento i en la inercia explicada por el factor.

λ_α es la inercia explicada por el eje α, $\lambda_\alpha = \sum f_{i.} F_\alpha^2(i)$

La fórmula que nos permitirá obtener dichos porcentajes es:

$$Cta(i,\alpha) = \frac{f_{i.}.coord^2(i,\alpha)}{\lambda_\alpha} = \frac{f_{i.}.F^2{}_\alpha(i)}{\lambda_\alpha}$$

Esta contribución está afectada no únicamente por su distancia al origen (centro de gravedad) o desviación de la media, sino que también se encuentra afectada por su peso.

Contribuciones relativas (Ctrα(I))

Expresan la contribución de un factor en la explicación de la dispersión de un elemento. Nos indica la calidad de representación de la modalidad. Las contribuciones relativas muestran cuales son las características exclusivas de ese factor. Mide la parte del punto (i,j) en la inercia explicada por el eje factorial.

Es decir, recoge la participación del factor α en la explicación del elemento i. Mide la calidad de representación de i sobre el eje α.

$$Ctr(i,\alpha) = \frac{coord^2(i,\alpha)}{d^2(i,O)} = \frac{F^2{}_\alpha(i)}{d^2(i,G)}$$

como:

$$d^2(i,G) = \sum_{j=1}^{q}\left(\frac{f_{ij}}{\sqrt{f_{.j}}f_{i.}} - \sqrt{f_{.j}}\right)^2$$

y cumple con la condición de que la suma de las contribuciones de todos los puntos (filas o columnas) es igual a la unidad.

$$\sum_{\alpha\in A} Ctr_\alpha(i) = 1$$

Las inercias

La parte de inercia debida a una modalidad de respuesta j es mayor cuanto menor sea el efectivo de esa modalidad. En efecto, si G representa el centro de gravedad, la inercia debida a la modalidad j es:

$$I(j) = f_{.j}d^2(j,G) = f_{j.}\sum_i\left(\frac{f_{ij}}{f_{.j}\sqrt{f_{i.}}} - \sqrt{f_{i.}}\right)^2 = \frac{n_{j.}}{nQ}\sum_i\left(\frac{n_{ij}\big/nQ}{k_{.j}[1/n]} - 1\big/\sqrt{n}\right)^2 = \frac{1}{Q}\left(1-\frac{n_{.j}}{n}\right)$$

En consecuencia, se recomienda desestimar las modalidades que son elegidas muy pocas veces (se construye otra modalidad uniéndola a la más próxima).

La parte de la inercia debido a una pregunta es función creciente del número de modalidades de respuesta que tiene. En efecto, la inercia de una pregunta es la suma de las inercias de sus modalidades.

$$I(J_k) = \sum_{j\in J_k} I(j) = \sum_{j\in J_k}\frac{1}{Q}\left(1-\frac{n_{.j}}{n}\right) = \frac{1}{Q}(m_k - 1) \qquad (2.27)$$

Si un número de pregunta tiene un número de modalidades demasiado grande, igual que en el caso en que su efectivo sea muy pequeño, entonces se recomienda realizar una reagrupación de las modalidades en un numero razonable y que continúe manteniendo el sentido para evitar influencias extremas. Si la intención es considerar la información entonces se debe proyectar como suplementarias las modalidades sin agruparlas.

La inercia total es la suma de las inercias de todas las preguntas

$$I = \sum_k I(J_k) = \sum_k \frac{1}{Q}(m_k - 1) = \frac{J}{Q} - 1 \qquad (2.28)$$

J/Q es el número medio de modalidades por pregunta. En consecuencia, la inercia total solo depende del número de modalidades por pregunta. En consecuencia, la inercia total depende del número de modalidades y de preguntas.

En general, en el análisis de la tabla disyuntiva Z (AFCM), las tasas de inercia de los ejes dan una idea pesimista de la información extraída por ellos. Debido a ello, para tener una imagen más realista de la importancia de cada eje en la explicación de la inercia total de las variables en estudio, y siguiendo la transformación propuesta por Benzécri (1979) obtenemos valores propios corregidos utilizando la fórmula de la expresión 2.xx. La transformación de Benzécri consiste en restar la inercia trivial (1/Q) a cada valor propio original que tendría si no existiera relación entre las variables.

$$u = \left(\lambda - \frac{1}{Q}\right)^2 \left(\frac{Q}{Q-1}\right)^2$$

donde λ es el valor propio original y Q el número de variables activas incluidas en el análisis. Esta transformación debe ser considerada con mucho cuidado al momento de interpretar los resultados.

Interpretación

Ésta se realizará de la misma manera y que se haría con el AFCS, pero siempre teniendo en consideración las características especiales de la inercia de este análisis.

En general, suele ser suficiente dos o tres ejes factoriales para estudiar la relación existente entre las modalidades contenidas en la variable fila como en la columna. Debemos ser conscientes de que el AFCS no nos mide la intensidad de la relación entre las variables, simplemente presenta asociaciones entre las categorías. A partir de la representación simultanea de los puntos fila y columna sobre el primer plano factorial formado por los dos primeros ejes que recogen la mayor cantidad de información expresada por el mayor porcentaje de inercia recogido.

En general podemos decir a la hora de interpretar que:

Si dos filas o columnas tienen una estructura semejante, su situación será próxima sobre el plano (hay que estudiar la calidad de la representación).

La situación cercana de un punto fila y un punto columna solo se pueden interpretar si están alejados del origen.

Cuando una fila tiene un comportamiento medio se encontrará aproxima al origen.

Asimismo, la interpretación de los ejes es fundamental, deberemos seguir una serie de pautas para evitar errores:

En primer lugar, se buscan aquellos puntos con mayor CTA. Estos serán los que contribuyen más a la construcción del eje.

Se tiene en cuenta cuál de ellos se oponen. Es decir, cuáles de ellos están situados en la parte positiva o negativa.

Se estudia la calidad de estos puntos (Contribuciones relativas). Si uno de los puntos contiene una contribución pequeña entonces se debe suponer que determina una participación importante en otra dimensión/eje.

CAPÍTULO III:
APLICACIÓN DEL ANALISIS DE CORRESPONDENCIAS MULTIPLES A UN ESTUDIO IMAGEN DE LAS PRINCIPALES MARCAS DE LA INDUSTRIA DE TECNOLOGÍAS DE LA INFORMACIÓN SOBRE SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES DEL PERÚ

3.1 Introducción

Los que dirigen las organizaciones del Perú están conscientes del problema que significa “cuidar” la información, en mayor magnitud aquella considerada como vital o de alta confidencialidad. Es por ello por lo que las medidas adoptadas en cuanto a la seguridad de esta información deben estar muy bien organizada y controlada mediante mecanismos adecuados.

Poco a poco se toma conciencia de que la inversión en la seguridad de la empresa es una medida primordial y que no hay esperar un ataque para reaccionar. Se debe ser proactivo y no reactivo ante las amenazas o ataques.

En tal sentido, es necesario conocer cuál es el estado actual de la seguridad en las organizaciones, conocer cuáles fueron los principales problemas y ataques detectados durante el 2005.

Las marcas vinculadas a los temas de seguridad informática en el Perú tienen mucho interés en investigar sobre este tema, para tener elementos que le permitan elaborar sus planes de marketing, estrategias para poder competir en el mercado de TI (Tecnologías de la Información) en el Perú.

Este trabajo servirá de base para aquellos alumnos, tesistas y público en general vinculados a la industria de Tecnologías de la Información en el Perú.

En virtud de estas razones explicadas, se realizó este estudio durante el mes de Noviembre del año 2006.

3.2 Diseño de la investigación

El método para utilizar en este trabajo es no experimental, es un estudio cuantitativo, transversal, descriptivo. Los resultados obtenidos en este trabajo de investigación están aceptados como válidos por la comunidad científica.

El método científico es el más adecuado para obtener resultados que den respuesta a los objetivos propuestos en este trabajo de investigación. Para tal fin, se utilizará lo siguiente:

Software estadístico SPSS 9.0 y Office XP

Población objetivo

La población está compuesta por las organizaciones que invierten o consumen en bienes o servicios de TI en el Perú sin contar las pequeñas y microempresas. El tamaño de la población se estima en 9,208 organizaciones tanto de gobierno, empresas corporativas, grandes empresas y medianas empresas.

Diseño muestral

Se trabajó de manera independiente cada segmento de la población y de casa uno de ellos se extrajo una muestra aleatoria simple y sin reposición. El cuadro que se muestra a continuación detalle le mencionado:

Segmento	Población	Muestra	Error esperado
Corporaciones y Grandes empresas	309	150	5.7%
Medianas empresas	8691	320	5.4%
Principales organizaciones de gobierno	208	120	5.8%
Total	**9208**	**590**	**3.9%**

Se utilizó la relación Error esperado y tamaño de muestra de un intervalo conservador (p=0.5), es decir, mediante la siguiente fórmula:

$$n = \frac{NPQ}{\left(\frac{d}{Z_a}\right) * (N-1) + PQ}$$

Metodología para la obtención de datos

Para la obtención de los datos necesarios en este estudio, primero se verificó un cuestionario previamente diseñado y aplicado en el 2003. Una vez aprobado el cuestionario por un grupo de especialistas en el tema tanto de elaboración y diseño de cuestionarios como especialistas en el mercado de TI.

Una vez elegida y aprobada la herramienta de recojo de información, se procedió a aplicar el cuestionario por un equipo de teleoperadoras previamente entrenadas tanto en la metodología a utilizar como en la operatividad del cuestionario.

Una vez aprobado un examen para poder contar con información calificada, se procedió a aplicar el cuestionario.

Unidad informante

Se designó como persona adecuada para brindar la información al máximo responsable del área de sistemas en las organizaciones elegidas en la muestra.

3.3 Análisis descriptivo de los datos

Se utilizó en gran medida estadística descriptiva para conocer el posicionamiento, participación de mercado de las diferentes marcas de la industria de TI.

Se calcularon porcentajes para obtener la participación de mercado y penetraciones

La diferencia entre participación y penetración radica en la modalidad de respuesta; mientras que para la participación de mercado calculada los porcentajes (participaciones de mercado) suman 100%, la penetración no suma necesariamente 100% ya que trabaja con respuestas múltiples.

Los resultados se presentan a manera general, es decir se muestra las participaciones y penetraciones de todos los segmentos juntos. Luego se aplicará la técnica de análisis factorial de correspondencias múltiples para poder visualizar de manera amplia todas las variables en estudios y en sus diferentes modalidades.

Podemos observar que la marca Cisco es la marca considerada como más segura seguida de IBM con 32% y 19% de penetración respectivamente (ver cuadro 84 del apéndice).

Esta consideración es absolutamente independiente a que, si la organización cuenta o no con alguna solución de seguridad de esta marca, es por eso por lo que las respuestas obtenidas están relacionadas con la "imagen" que poseen las marcas.

Se puede observar que, en cuanto a seguridad física, llámese seguridad ante incendios, terremotos, aire acondicionado, pozo a tierra, etc. un alto porcentaje de organizaciones cuentan con las medidas y mecanismos necesarios para poder estar seguros ante cualquiera estos ataques (ver cuadros 2 al 10 del apéndice).

En lo que se refiere a UPS, un 98% de organizaciones cuentan con esta máquina, a pesar de lo relativamente costoso que pueda significar (ver cuadro 6 del apéndice). En este sentido, la marca que ha logrado una buena participación en la base instalada de estos UPS es APC (46% de penetración en las organizaciones) seguida muy de lejos de Powercom con un 6% de penetración en las organizaciones (ver cuadro 7 del apéndice).

En lo que se refiere a seguridad lógica, comenzaremos por mencionar que en términos generales la seguridad en las organizaciones es buena.

Podemos notar que la gran mayoría de organizaciones emplean software antivirus, casi la mitad de las organizaciones emplean software anti troyanos y antispyware (ver cuadros 12 y 33 del apéndice). Se puede notar que Mc Afee tiene la mayor penetración en los softwares antispyware instalados en casi la mitad de las organizaciones, seguido de AdAware con una penetración de 11% (ver cuadro 34 del apéndice).

En cuanto al conocimiento de términos como antivirus, antispyware, antiadware y demás mostrados en el apéndice es muy alto salvo en los casos de phishing y pharming. Es necesario notar que la gran mayoría de organizaciones menciona no haber sufrido ataques de pharming ni de phishing sin embrago la gran mayoría de organizaciones menciona no conocer sobre estos términos (ver cuadros 63 al 83 del apéndice).

Observamos que la gran mayoría de organizaciones tienen implementado firewall y antispam (ver cuadros 27 y 30 del apéndice); sin embargo, una cantidad muy reducid de organizaciones cuentan con alguna solución de IDS / IDP (ver cuadro 32 del apéndice).

El nivel de compromiso en temas de seguridad es bastante alto tanto por parte de la alta dirección, usuarios y personal de sistemas de las organizaciones en estudio (ver cuadro 49 del apéndice).

En cuanto a los presupuestos para la seguridad de las organizaciones, un 47.7% menciona que se incrementó del 2003 al 2005, y un 73.3% de organizaciones piensan que éste debería seguir incrementándose (ver cuadro 50 del apéndice).

En temas de políticas de seguridad, estándares de seguridad, Líneas de base de seguridad, Líneas de guía de seguridad y Procedimientos de

seguridad, más de la mitad de las organizaciones cuentan con ello (ver cuadros del 40 al 45 del apéndice).

Poco más de la mitad de las organizaciones realizan auditoria en sus sistemas de seguridad ya sea externa o interna (ver cuadro 89 del apéndice).

Finalmente podemos notar que, en temas de tercerización, la dinámica de este mercado está aún en proceso de fortalecimiento, esto debido a la tendencia en las empresas y organizaciones en tercerizar sus servicios o procesos para reducir sus costos de operación, ganar mayor eficiencia, entre otros. Sólo un 6.6% de organizaciones entrevistadas tienen algún servicio de seguridad mercerizado (ver cuadro 90 del apéndice).

3.4 Aplicación del Análisis de Correspondencias Múltiples

En cuanto al análisis factorial de correspondencias múltiples aplicado para determinadas variables a criterio del investigador, se puede observar lo siguiente:

El autovalor calculado para la primera dimensión es 0.1638 mientras que el segundo es de 0.0988. Esto nos quieres decir que el primer factor explica en mejor magnitud la varianza total mientras que la segunda dimensión se encuentra algo lejos sin embargo utilizaremos las dos dimensiones para poder tener mejores elementos de comparación.

Para la formación de la primera dimensión, las variables: Tenencia de políticas, estándares, líneas de base, líneas de guía y procedimientos en seguridad son las más importantes. Esto debido a que tienen el mayor valor de las medidas de discriminación reflejado en el cuadro contenido en el anexo. Análogamente notamos que las variables más importantes en la formación de la segunda dimensión son: tenencia de software antispyware y antiadware.

En cuanto a los cuadrantes observamos lo siguiente:

El primer cuadrante caracteriza a las organizaciones que tienen una elevada base instalada de desktops, notebooks y servidores, aquellas organizaciones que usan firmas y certificados digitales, organizaciones

que emplean software antiadware, antispyware y anti troyanos, y por último a las organizaciones que emplean IDS / IDP.

El segundo cuadrante caracteriza a las organizaciones que no poseen políticas, estándares, líneas de base, líneas de guía y procedimientos en seguridad, aquellas organizaciones que no poseen UPS, extintores ni IDS / IDP.

El tercer cuadrante caracteriza a las organizaciones que no tienen aire acondicionado, no usan portátiles, firewalls, no usan software antispyware, no usan software antiadware, no usan certificados digitales. Además, también a las organizaciones con mínima base instalada de desktops y que no realizan medición del impacto de un ataque a la seguridad de su organización.

El cuarto cuadrante caracteriza a las organizaciones que, si poseen políticas, estándares, líneas de guía, líneas de base y procedimientos en seguridad. Además, también a las organizaciones que si poseen supresores de pico en su área de cómputo.

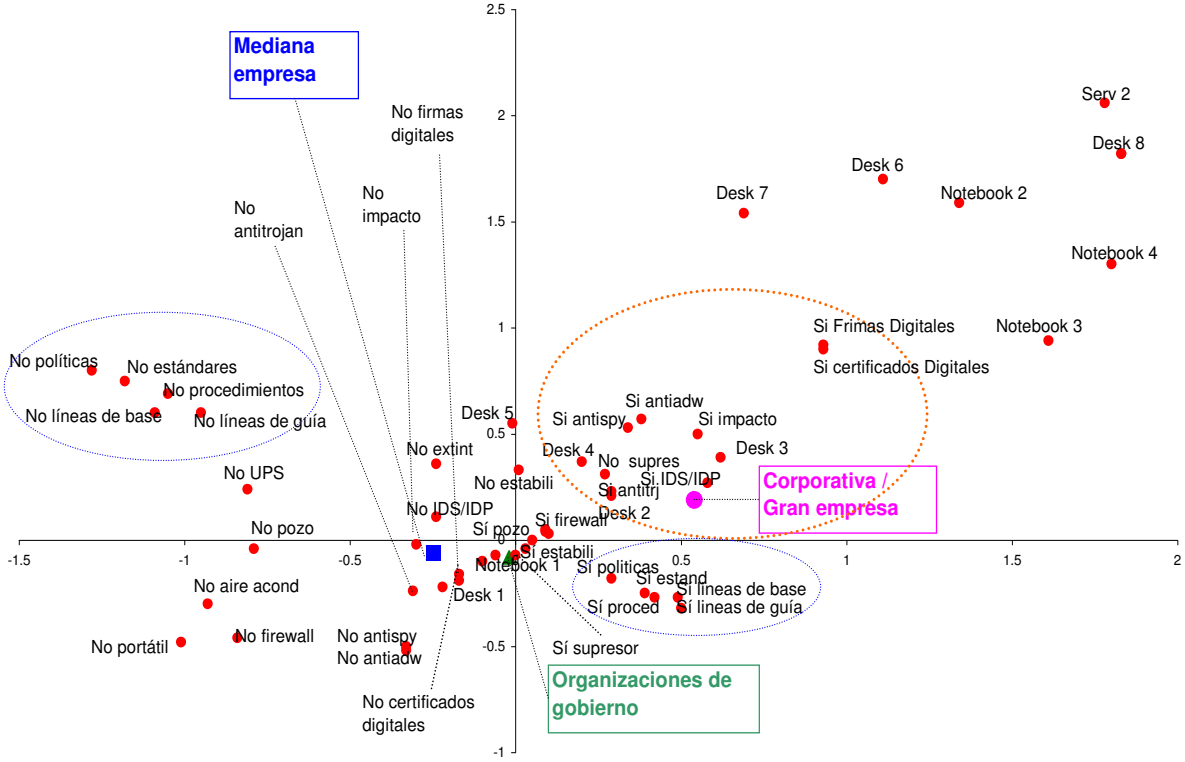
Podemos observar también que en cuanto a las organizaciones caracterizadas en función al segmento al cual pertenece lo siguiente:

Las empresas grandes y corporativas se caracterizan por tener una elevada base instalada de desktops, notebooks y servidores; además de usar software antitroyanos, antispyware y antiadware. También caracteriza a las empresas que usan IDS / IDP, usan firmas y certificados digitales además de usar firewalls.

Las empresas medianas se caracterizan por no usar software antitroyanos, no usan firmas ni certificados digitales, no realizan mediciones del impacto que pudiera ocasionar un ataque a su seguridad. Aquellas empresas también que no emplean IDS / IDP y tienen una cantidad menor de base instalada de desktops y notebooks.

Las organizaciones de gobierno son un caso específico, ya que si bien es cierto no está bien representada en el mapa de dos dimensiones, es probable que si lo esté en una tercera dimensión y esté relacionada con las variables que están cerca de ella. Es decir que, si poseen pozo a tierra, estabilizadores; sin embargo, no usan firmas ni certificados digitales.

El siguiente mapa perceptual generado por el análisis de correspondencias múltiples nos ilustra de manera gráfica lo mencionado:



CONCLUSIONES

En general, se pudo observar que, si bien las organizaciones en estudio están empezando a tomar mayor conciencia en temas de seguridad, esto gracias a comparaciones con el estudio similar desarrollado en el 2003 a la misma población objetivo, existe aún barreras para las empresas medianas y organizaciones de gobierno debido quizás a presupuestos o concientización de los responsables en este tema en las organizaciones. Esto debido a los resultados obtenidos:

1. un 47.7% de organizaciones mencionaron que su presupuesto en seguridad informática se incrementó desde el año 2001 hasta el 2005, y un 73.3% de organizaciones opinan (el gerente de sistemas) que el presupuesto destinado para la seguridad informática debería incrementarse aún más.

   Esto es una muy buena noticia ya que nos refleja una tendencia a mejorar los niveles de seguridad ya sea física y lógica en las organizaciones. Esto significa más presupuesto, más mercado, más demanda y más competencia.
2. En cuanto a la caracterización de las organizaciones descrita anteriormente, cabe mencionar que las organizaciones de gobierno se caracterizan más por poseer pozo a tierra, estabilizador y supresor, esto puede explicarse debido a la íntima relación que tienen con las organizaciones gubernamentales encargadas de regular estas medidas de seguridad.
3. Las empresas grandes y corporativas realizan esfuerzos mayores, no significando que un porcentaje de estas empresas no posean pozo a tierra ni estabilizador de voltaje ni supresor de pico, en resguardar la seguridad lógica. Esto puede explicarse debido a la naturaleza en si del mercado. En un mercado de competencia la información es muy valiosa y si cae o es violada por entes o personas de la competencia será desastroso. Es por eso por lo que existe también una tendencia en no poseer mucho notebook, esto se puede notar en al mapa perceptual, las grandes empresas y corporativas si poseen más notebooks que las demás organizaciones, pero se caracterizan más

por las variables que están más cercanas a él (ver mapa perceptual), esto debido a que existe un cierto temor en que la información contenida en una notebook está muy expuesta y la consideran en riesgo.

4. El conocimiento y preocupación en temas de seguridad es muy alentador, esto favorecerá tanto a las marcas en el mercado de TI como a los usuarios.

SUGERENCIAS

1. De la información que se ha podido obtener con éste estudio, podemos sugerir a las empresas dedicadas a la comercialización de software/hardware para la seguridad física y lógica que se cuenta con una creciente preocupación por éstos temas en las organizaciones mencionadas y que además, las personas con cargos de responsabilidad respecto a éstos temas están conscientes que se debería aumentar el presupuesto destinado para la adquisición de software de seguridad informática y también equipos para la seguridad física como extintores, UPS, entre otros.
2. Es notable también sugerir una mayor difusión o encontrar el canal adecuado para cada segmento; en especial a las organizaciones de gobierno y medianas empresas para la actualización de amenazas para la seguridad lógica ya que, según los resultados presentados, existe un alto porcentaje de encargados de sistemas o análogos que desconocen por ejemplo las amenazas de “pharming”, “phishing” y “keyloggers”.
3. Pensamos que es el momento para poder madurar mejor una oferta de valor en temas como estos por partes de las empresas ofertantes y, para los consumidores un momento especial en aprovechar el desarrollo competitivo del mercado y encontrar la oferta que más se adecue a sus proyectos en seguridad.

GLOSARIO DE TÉRMINOS

ADWARE, programa que automáticamente se ejecuta, muestra o baja publicidad web al computador después de instalar el programa o mientras se está utilizando la aplicación.

APC, American Power Conversion es una empresa que proporciona protección contra una de las principales causas de pérdida de datos, daños en hardware y tiempo de inactividad: los problemas del suministro eléctrico.

CISCO, Cisco Systems, Inc. es una empresa líder mundial en redes para Internet. Se dedica al desarrollo de tecnologías de conectividad basadas en el Protocolo de Internet (IP).

ESTABILIZADOR DE CORRIENTE, es un instrumento que permite brindar una salida de voltaje estable sea cual sea el voltaje de entrada.

FIREWALL, Existe en una red o sistema y cuyo objetivo es brindar seguridad permitiendo o no el acceso a los mismos. Asimismo, permite la comunicación autorizada y segura aplicando el cifrado y descifrado de las comunicaciones.

GUSANOS, se parecen a los virus informáticos con la diferencia que no necesitan de la intervención del ser humano para atacar. Su ataque se manifiesta en su capacidad de duplicarse a gran escala. Son llamados también IWorm.
Los gusanos informáticos radican en la memoria del computador y no atacan archivos, sino que se multiplican.

IDS/IDP, el sistema de detección de intrusos y el sistema de prevención de intrusos respectivamente permiten identificar incidentes y/o ataques que puedan afectar la seguridad de un sistema/red. Esta información llega al responsable de la seguridad.

KEYLOGGER, es un dispositivo ya sea software/hardware que captura las pulsaciones que se realizan en el teclado para luego guardar estos registros en algún dispositivo de almacenamiento o dirigirlas a algún sitio web.

MALWARE, es aquel código/software que tiene por objetivo infiltrarse en algún sistema/dispositivo/red y causar daños.

OUTSOURCING, acción mediante la cual se contrata el servicio de ejecución de algunas actividades y/o procesos brindadas por una organización ajena.

PHARMING, es el ataque a una debilidad del software/aplicaciones de los servidores DNS (Domain Name System) y que también puede darse en los equipos de los usuarios, y consiste en cambiar de dirección a un nombre de dominio (domain name) a otra dirección. De esta forma, un usuario que ingrese a alguna dirección web desde su computadora/equipo y que esta dirección haya sido atacada mediante pharming en realidad estará ingresando a la dirección que el atacante haya definido. Todo esto, haciendo que el diseño de la página o sitio web atacado se parezca mucho visualmente a la verdadera.

PHISHING, es aquel ataque basado en ingeniería social el cual tiene por objetivo capturar ilegalmente información confidencial logrando captar la confianza de la víctima. Uno de los canales utilizado en mediante correo electrónico haciendo creer que se trata de una entidad conocida y confiable y mediante esa confianza que lograr captar en ese momento es que lograr obtener información del usuario.

SPAM, llamados también correo basura y que son comunicaciones que no fueron solicitados ni deseados que simplemente son de remitentes desconocidos y que de alguna manera generan malestar al usuario/víctima.

SPYWARE, conocido también como software espía y que en sí realiza dicha función. Recopila información de un equipo/computadora y la envía a destinatarios específicos definidos por el atacante sin que éste lo haya autorizado.

SUPRESOR DE PICOS, es un equipo que mantiene constante los voltajes que pudieran ser elevados repentinamente.

TECNOLOGÍAS DE LA INFORMACIÓN, Es aquella actividad que contempla el estudio del almacenaje, protección, conversión, procesamiento, transmisión y recuperación de la información.

TROYANO, es aquel software o código que se manifiesta al usuario/víctima como inofensivo pero que al ejecutarlo le brinda accesos al atacante con fines maliciosos/no permitidos.

UPS, es un dispositivo/equipo destinado a brindar energía eléctrica por un reducido tiempo ante un corte inesperado de suministro eléctrico con el fin de dar tiempo a los usuarios para salvaguardar la información que esté sin guardar o la culminación o gestión de procesos que aún se estén ejecutando. Básicamente le brinda algo de tiempo al usuario para que realice las acciones necesarias ante un corte de energía eléctrica.

VIRUS INFORMATICO, son archivos ejecutables que usualmente reemplazan a los originales y que tienen el fin de causar daños a la información guardada en el ordenador o afectar a los sistemas del ordenador o simplemente causar una broma al usuario. Cabe mencionar que, a diferencia de los gusanos informáticos, éstos no pueden multiplicarse a sí mismos.

Bibliografía

(s.f.). Obtenido de correo.tulum.gob.mx

BAN Biblioteca Agraria Nacional. (s.f.). Obtenido de http://tumi.lamolina.edu.pe/ban/

CYBERTESIS. (s.f.). Obtenido de www.cybertesis.unmsm.edu.pe

Docplayer. (s.f.). Obtenido de www.docplayer.es

Dominio Consultores. (s.f.). Obtenido de www.dominio-consultores.com

Dominio Consultores. (2003). *Estudio de Seguridad Informática en Marketing organizaciones del Perú.* Perú.

Dominio Consultores. (2006). *Informe del mercado peruano de cómputo en Marketing Inversiones y Tendencias 2005-2006.*

Johnson, D. E. (1998). *Métodos Multivariados aplicados al análisis de datos.* México: Internacional Thomson.

La Molina. (s.f.). Obtenido de www.lamolina.edu.pe

Oré, C. G. (2002). *Métodos estadísticos en la evaluación educacional.* Perú: Concytec.

Schemelks, C. (1988). *Manual para la presentación de anteproyectos e informes de investigación (tesis).* México: Harla.

SPOL. (s.f.). Obtenido de www.dspace.espol.edu.ec

Trout, A. R. (1994). *Las 22 leyes inmutables del marketing.* México: McGraw-Hill Interamericana.

ULPGC. (s.f.). Obtenido de www.fcee.ulpgc.es

Universidad de Málaga. (s.f.). *UMA.ES*. Obtenido de https://riuma.uma.es/

UNIVERSITAT DE BARCELONA. (s.f.). Obtenido de www.bio.ub.es

APÉNDICE

Muestra obtenida

Cuadro 1

Segmento	Frecuencia	Distrib. Porcentual
Grande / Corporativa	153	25%
Mediana	325	54%
Gobierno	125	21%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que tienen extintores en el área de cómputo

Cuadro 2

Tenencia de extintores	Frecuencia	Distrib. Porcentual
Sí tiene	527	87%
No tiene	76	13%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que tienen sensores contra incendios en el área de cómputo

Cuadro 3

Tenencia de sensores contra incendios	Frecuencia	Distrib. Porcentual
Sí tiene	254	42%
No tiene	349	58%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que usan supresores de pico en el área de cómputo

Cuadro 4

Uso de supresores de pico	Frecuencia	Distrib. Porcentual
Sí usan	489	81%
No usan	114	19%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que utilizan estabilizadores de voltaje en el área de cómputo

Cuadro 5

Utilización de estabilizadores de voltaje	Frecuencia	Distrib. Porcentual
Sí utilizan	501	83%
No utilizan	102	17%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que utilizan UPS en el área de cómputo

Cuadro 6

Utilización de UPS	Frecuencia	Distrib. Porcentual
Sí utilizan	589	98%
No utilizan	14	2%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Penetración de las marcas de UPS utilizadas en el área de cómputo

Cuadro 7

Marca de UPS que utilizan las organizaciones	Frecuencia	Distrib. Porcentual
APC	214	46%
Powercom	26	6%
Tripplite	24	5%
Gamatronic	23	5%
Liebert	22	5%
PowerWare	18	4%
Emerson	17	4%
Otras marcas	159	Menos de 4%
Total	464	
No sabe / No recuerda	125	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que cuentan con aire acondicionado en el área de cómputo

Cuadro 8

Tenencia de aire acondicionado	Frecuencia	Distrib. Porcentual
Organizaciones que sí tienen	536	89%
Organizaciones que no tienen	67	11%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que cuentan con pozo a tierra

Cuadro 9

Tenencia de pozo a tierra	Frecuencia	Distrib. Porcentual
Organizaciones que sí tienen	571	95%
Organizaciones que no tienen	32	5%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Cuadro 10

Tenencia de pozo a tierra	Sí tienen	Total	2003
Extintores	87%	603	(*)
Sensores contra incendios	42%	603	32%
Supresores de pico	81%	603	84%
Estabilizadores de voltaje	83%	603	86%
UPS	98%	603	85%
Aire acondicionado	89%	603	(*)
Pozo a tierra	95%	603	(*)

(*) No se investigó en el 2,003

Organizaciones que usan software antivirus

Cuadro 11

Uso de software antivirus	Frecuencia	Distrib. Porcentual

Organizaciones que sí usan	601	99.7%
Organizaciones que no usan	2	0.3%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que usan software antitroyanos

Cuadro 12

Uso de software antitroyanos	Frecuencia	Distrib. Porcentual
Organizaciones que sí usan	309	51.4%
Organizaciones que no usan	292	48.6%
Total	601	100%
Confidencial	2	

La tabla expresa en cantidad el número de organizaciones

Modalidad de actualización del Sistema operativo

Cuadro 13

Actualización del Sistema Operativo	Frecuencia	Distrib. Porcentual
Automática	362	60%
Manual	168	28%
Cada vez que sale una actualización	69	11%
No realiza	3	0.5%
Total	602	100%

Confidencial 1

La tabla expresa en cantidad el número de organizaciones

Modalidad de actualización de las aplicaciones de comunicaciones

Cuadro 14

Actualización de aplicaciones de comunicaciones	Frecuencia	Distrib. Porcentual
Automática	323	54%
Manual	189	32%
Cada vez que sale una actualización	63	11%
No realiza	25	4.2%
Total	600	100%

Confidencial 3

La tabla expresa en cantidad el número de organizaciones

Modalidad de actualización del browser

Cuadro 15

Actualización del Browser	Frecuencia	Distrib. Porcentual
Automática	320	53%
Manual	195	33%
Cada vez que sale una actualización	58	10%
No realiza	27	4.5%
Total	600	100%

Confidencial 3

La tabla expresa en cantidad el número de organizaciones

Modalidad de actualización de las aplicaciones de productividad

Cuadro 16

Actualización de aplicaciones de productividad	Frecuencia	Distrib. Porcentual
Manual	267	45%
Automática	246	41%
Cada vez que sale una actualización	64	11%
No realiza	22	3.7%
Total	599	100%

Confidencial 4

La tabla expresa en cantidad el número de organizaciones

Organizaciones que realizan backups o copias de respaldo

Cuadro 17

Realización de backups y/o copias de respaldo	Frecuencia	Distrib. Porcentual
Organizaciones que sí lo realizan	590	97.8%
Organizaciones que no lo realizan	13	2.2%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Lugar donde se guardan los backups o copias de respaldo

Cuadro 18

Lugar donde se guardan las copias backups	Frecuencia	Distrib. Porcentual
Misma compañía	165	28%
Lugar externo	165	28%
Ambos	254	43.5%
Total	584	100%
Confidencial	6	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que cuentan con solución de Disaster Recovery

Cuadro 19

Implementación de solución Disaster Recovery	Frecuencia	Distrib. Porcentual
Sí tienen implementado	184	31%
No tienen implementado	419	69%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que usan firmas digitales

Cuadro 20

Uso de firmas digitales	Frecuencia	Distrib. Porcentual
Sí usan	98	16%
No usan	505	84%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que usan certificados digitales

Cuadro 21

Uso de certificados digitales	Frecuencia	Distrib. Porcentual
Sí usan	115	19%
No usan	488	81%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que almacenan y monitorean los correos electrónicos de los usuarios

Cuadro 22

Almacenamiento y monitoreo de correos electrónicos de usuarios	Frecuencia	Distrib. Porcentual
Sí lo realizan	346	58%
No lo realizan	253	42%
Total	599	100%
Confidencial	4	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que emplean filtros de contenido

Cuadro 23

Empleo de filtros de contenido	Frecuencia	Distrib. Porcentual
Sí lo emplean	430	72%
No lo emplean	171	28%
Total	601	100%
Confidencial	2	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que guardan copias de password de sus usuarios en lugar seguro

Cuadro 24

Guardado de copias de passwords de usuarios	Frecuencia	Distrib. Porcentual
Sí lo realizan	316	53%
No lo realizan	281	47%
Total	597	100%
Confidencial	6	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que tienen servidor de archivos

Cuadro 25

Tenencia de servidor de archivos	Frecuencia	Distrib. Porcentual
Sí tienen	508	84%
No tienen	95	16%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que emplean notebooks

Cuadro 26

Tenencia de notebooks en la organización	Frecuencia	Distrib. Porcentual
Sí tienen	534	89%
No tienen	69	11%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Organizaciones que emplean firewalls para asegurar la red

Cuadro 27

Empleo de firewalls	Frecuencia	Distrib. Porcentual
Sí lo emplean	523	87%
No lo emplean	78	13%
Total	601	100%
Confidencial	2	

La tabla expresa en cantidad el número de organizaciones

Penetración de las marcas de firewalls en las organizaciones

Cuadro 28

Marcas de firewalls	Frecuencia	Penetración
Linux	204	39.0%
Cisco	52	10.0%
Isa Server	21	4.0%
Check Point	16	3.0%
Juniper	10	2.0%
Microsoft	10	2.0%
Otros	Menos de 10	Menos de 2%
Total	523	
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Monitoreo de los firewalls utilizados por las organizaciones

Cuadro 29

Monitoreo del firewall	Frecuencia	Distrib. Porcentual
Entrada de datos	52	9.9%
Salida de datos	3	0.6%
Ambos	463	88.3%
No sabe	5	1.0%
Total de casos	523	100%
Confidencial	1	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que emplean software anti-spam

Cuadro 30

Empleo de software anti-spam	Frecuencia	Distrib. Porcentual
Sí lo emplean	366	61%
No lo emplean	232	39%
No sabe	2	0.3%
Total	600	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Lugar donde se encuentra instalado el anti-spam en las organizaciones que lo poseen

Cuadro 31

Lugar de instalación del software anti-spam	Frecuencia	Penetración
Servidor	274	75.5%
Ambos	75	20.7%
Estaciones	17	4.7%
No sabe	4	1.1%
Appliance	1	0.3%
Local Principal	1	0.3%
Total	363	
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que usan IDS / IDP

Cuadro 32

Uso de IDS / IDP	Frecuencia	Distrib. Porcentual
Sí lo usan	182	30%
No lo usan	420	70%
Total	602	100%
Confidencial	1	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que Emplean algún software anti-spyware

Cuadro 33

Empleo de software anti-spyware	Frecuencia	Distrib. Porcentual
Sí lo emplean	288	48%
No lo emplean	313	52%
Total	601	100%
Confidencial	2	

La tabla expresa en cantidad el número de organizaciones

Penetración de la marca de anti-spyware

Cuadro 34

Marca de anti-spyware que utilizan las organizaciones	Frecuencia	Penetración
McAfee	61	24%
AdAware	27	11%
Panda	26	10%
TrendMicro	22	9%
Linux	17	7%
Microsoft	17	7%
Symantec	15	6%
Otras marcas	69	Menos de 6%
Total de casos	250	
No sabe / Confidencial	38	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que Emplean algún software anti-adware

Cuadro 35

Empleo de software anti-adware	Frecuencia	Distrib. Porcentual
Sí lo emplean	272	45%
No lo emplean	329	55%
Total	601	100%
Confidencial	2	

La tabla expresa en cantidad el número de organizaciones

Penetración de la marca de anti-adware

Cuadro 36

Marca de anti-adware que utilizan las organizaciones	Frecuencia	Penetración
McAfee	56	23%
AdAware	31	13%
No sabe	24	10%
Panda	22	9%
TrendMicro	21	9%
Microsoft	17	7%
Norton	15	6%
Otras marcas	77	Menos de 6%
Total de casos	240	
No sabe / Confidencial	32	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que tienen red inalámbrica

Cuadro 37

Tenencia de red inalámbrica	Frecuencia	Distrib. Porcentual
Sí tienen	242	40%
No tienen	360	60%
Total	602	100%
Confidencial	1	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que encriptan el Messenger

Cuadro 38

Encriptación del messenger	Frecuencia	Distrib. Porcentual
Sí lo encriptan	87	14%
No lo encriptan	516	86%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Cuadro 39

	Organizaciones que usan	2003
SW Anti-spam	61%	17%
SW Anti-spyware	48%	5%
SW Anti-virus	100%	99%
SW Anti-troyanos	51%	28%
SW Anti-adware	45%	5%
Disater recovery	31%	18%
Filtros de contenido	72%	(*)
Firewall	87%	50%
IDS / IDP	30%	(*)

(*) No se investigó en el 2,003

Organizaciones que cuentan con políticas de seguridad

Cuadro 40

Existencia de políticas de seguridad	Frecuencia	Distrib. Porcentual
Sí existen	493	82.4%
No existen	99	16.6%
Recién se está implementando	6	1.0%
Total	598	100%
Confidencial	5	

La tabla expresa en cantidad el número de organizaciones

Una “política de seguridad” es un documento estratégico que define el alcance de la seguridad requerida por una organización en términos de metas, misión, objetivos y propósitos. Es un documento de largo plazo y demuestra el compromiso con la seguridad de la alta gerencia

Cuadro 41

	Si existen	No existen	Recien se està implementando	Total respuesta *	No respuesta**	Total muestra	2003***
Tenencia de politicas de seguridad	82%	17%	1%	598	5	603	57%
Tenencia de estàndares en seguridad	73%	26%	1%	598	5	603	51%
Tenencia de lineas de base en seguridad	67%	32%	1%	598	5	603	35%
Tenencia de lineas de guìa en seguridad	64%	35%	1%	598	5	603	32%
Tenencia de procedimientos en seguridad	71%	28%	1%	598	5	603	45%

* Total respuesta significa el total de organizaciones que respondieron a las preguntas referidas a los temas mostrados.

** Se refiere a las organizaciones que no respondieron a estas preguntas por razones de confidencialidad.

** Son los resultados del estudio similar realizado en el 2003.

Organizaciones que cuentan con estándares de seguridad

Cuadro 42

Existen estándares de seguridad	Frecuencia	Distrib. Porcentual
Sí existen	437	73.1%
No existen	155	25.9%
Recién se está implementando	6	1.0%
Total	598	100%
Confidencial	5	

La tabla expresa en cantidad el número de organizaciones

Los “estándares” definen los requerimientos compulsivos de seguridad de una organización, el tipo de tecnología a emplear y el modo de implementación

Organizaciones que cuentan con Líneas de base de seguridad

Cuadro 43

Existen líneas de base de seguridad	Frecuencia	Distrib. Porcentual
Sí existen	401	67.1%
No existen	191	31.9%
Recién se está implementando	6	1.0%
Total	598	100%
Confidencial	5	

La tabla expresa en cantidad el número de organizaciones

Las “líneas de base” salen directamente de los estándares y son un grupo específico de requerimientos de seguridad que todos los sistemas de la organización deben cumplir o exceder

Organizaciones que cuentan con líneas de guía de seguridad

Cuadro 44

Existen líneas de guía de seguridad	Frecuencia	Distrib. Porcentual
Sí existen	380	63.5%
No existen	211	35.3%
Recién se está implementando	7	1.2%
Total	598	100%
Confidencial	5	

La tabla expresa en cantidad el número de organizaciones

Las "líneas de guía" son manuales operativos que definen el modo en que deben implementarse los estándares y las líneas de base. Reglamentan las condiciones para las alteraciones específicas de las líneas de base, prescriben metodologías y sugieren soluciones específicas para implementar la seguridad.

Organizaciones que cuentan con procedimientos de seguridad

Cuadro 45

Existencia de procedimientos de seguridad	Frecuencia	Distrib. Porcentual
Sí existen	423	70.7%
No existen	169	28.3%
Recién se está implementando	6	1.0%
Total	598	100%
Confidencial	5	

La tabla expresa en cantidad el número de organizaciones

Los “procedimientos” son documentos detallados que explican paso a paso cómo implementar los mecanismos de seguridad definidos en los documentos superiores. Son específicos a una plataforma, sistema operativo, software o mecanismo de seguridad.

Opinión sobre el estado de la seguridad a fines del 2005

Cuadro 46

Opinión sobre el estado de la seguridad en el 2005	Frecuencia	Distrib. Porcentual
Dramáticamente menos efectiva	27	4.6%
Algo menos efectiva	250	42.2%
Mas o menos igual	171	28.8%
Algo más efectiva	107	18.0%
Dramáticamente más efectiva	38	6.4%
Total	593	100%
Confidencial	10	

La tabla expresa en cantidad el número de organizaciones

Opinión sobre el nivel de compromiso de la alta dirección en temas de seguridad

Cuadro 47

Compromiso de la alta dirección	Frecuencia	Distrib. Porcentual
Nada comprometido	23	3.9%
Medianamente comprometido	60	10.1%
Totalmente comprometido	513	86.1%
Total	596	100%
Confidencial	7	

La tabla expresa en cantidad el número de organizaciones

Opinión sobre el compromiso del usuario en temas de seguridad

Cuadro 48

Compromiso del personal usuario	Frecuencia	Distrib. Porcentual
Nada comprometido	45	7.6%
Medianamente comprometido	127	21.3%
Totalmente comprometido	424	71.1%
Total	596	100%
Confidencial	7	

La tabla expresa en cantidad el número de organizaciones

Opinión sobre el nivel de compromiso del personal de sistemas en temas de seguridad

Cuadro 49

Compromiso del personal de sistemas	Frecuencia	Distrib. Porcentual
Nada comprometido	14	2.4%
Medianamente comprometido	28	4.7%
Totalmente comprometido	553	92.9%
Total	595	100%
Confidencial	8	

La tabla expresa en cantidad el número de organizaciones

Variación del presupuesto de seguridad antes del 2005

Cuadro 50

Variación del presupuesto antes del 2005 en seguridad	Frecuencia	Distrib. Porcentual
Incrementó	285	47.7%
Mantuvo	237	39.6%
Redujo	40	6.7%
No existe presupuesto	5	0.8%
No sabe	31	5.2%
Total	598	100%
Confidencial	5	

La tabla expresa en cantidad el número de organizaciones

Cuadro 51

Presupuestos para seguridad en las organizaciones

Variación del presupuesto para seguridad	Antes del 2,005	Deseado para el 2,006
Incremento	48%	73%
Decremento	7%	1%
Se mantuvo	40%	24%
No existe presupuesto	1%	0%
No sabe	5%	2%

Organizaciones que realizan medición del impacto de algún ataque a su seguridad

Cuadro 52

Medición del impacto de un ataque a la seguridad de la organización	Frecuencia	Distrib. Porcentual
Sí ha realizado	231	39%
No ha realizado	368	61%
Total	599	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad ante terremotos

Cuadro 53

Calificación de la seguridad ante terremotos	Frecuencia	Distrib. Porcentual
Nada vulnerable	295	50.3%
Medianamente vulnerable	156	26.6%
Muy vulnerable	136	23.2%
Total	587	100%
Confidencial	16	

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad ante incendios

Cuadro 54

Calificación de la seguridad ante incendios	Frecuencia	Distrib. Porcentual
Nada vulnerable	314	53.2%
Medianamente vulnerable	160	27.1%
Muy vulnerable	116	19.7%
Total	590	100%
Confidencial	13	

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad ante asaltos o robos

Cuadro 55

Calificación de la seguridad ante asaltos o robos	Frecuencia	Distrib. Porcentual
Nada vulnerable	352	59.7%
Medianamente vulnerable	122	20.7%
Muy vulnerable	116	19.7%
Total	590	100%
Confidencial	13	

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad en detección de intrusos en la red

Cuadro 56

Calificación de la seguridad en detección de intrusos en la red	Frecuencia	Distrib. Porcentual
Nada vulnerable	350	59.2%
Medianamente vulnerable	120	20.3%
Muy vulnerable	121	20.5%
Total	591	100%

Confidencial 12

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad en prevención de intrusos en la red

Cuadro 57

Calificación de la seguridad en la prevención de intrusos en la red	Frecuencia	Distrib. Porcentual
Nada vulnerable	350	59.2%
Medianamente vulnerable	121	20.5%
Muy vulnerable	120	20.3%
Total	591	100%

Confidencial 12

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad en passwords

Cuadro 58

Calificación de la seguridad en los passwords	Frecuencia	Distrib. Porcentual
Nada vulnerable	349	59.2%
Medianamente vulnerable	131	22.2%
Muy vulnerable	110	18.6%
Total	590	100%

Confidencial 13

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad en prevención de virus

Cuadro 59

Calificación de la seguridad en prevención de virus	Frecuencia	Distrib. Porcentual
Nada vulnerable	372	62.9%
Medianamente vulnerable	104	17.6%
Muy vulnerable	115	19.5%
Total	591	100%

Confidencial 12

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad en protección de datos

Cuadro 60

Calificación de la seguridad en protección de datos	Frecuencia	Distrib. Porcentual
Nada vulnerable	378	64.1%
Medianamente vulnerable	91	15.4%
Muy vulnerable	121	20.5%
Total	590	100%
Confidencial	13	

La tabla expresa en cantidad el número de organizaciones

Opinión de la seguridad ante robos de computadoras

Cuadro 61

Calificación de la seguridad ante robos de computadoras	Frecuencia	Distrib. Porcentual
Nada vulnerable	342	58.7%
Medianamente vulnerable	131	22.5%
Muy vulnerable	110	18.9%
Total	583	100%
Confidencial	20	

La tabla expresa en cantidad el número de organizaciones

Opinión sobre el futuro presupuesto para temas de seguridad

Cuadro 62

Opinión sobre la inversión futura en seguridad	Frecuencia	Distrib. Porcentual
Incrementar	436	73.3%
Mantener	143	24.0%
Disminuir	5	0.8%
No sabe	11	1.8%
Total	595	100%

Confidencial 8

La tabla expresa en cantidad el número de organizaciones

Conocimiento de Spam

Cuadro 63

Nivel de conocimiento de spam	Frecuencia	Distrib. Porcentual
Sí lo conoce	578	96.0%
No lo conoce	15	2.5%
Lo ha escuchado pero no lo conoce	9	1.5%
Total	602	100%

Confidencial 1

La tabla expresa en cantidad el número de organizaciones

Conocimiento de spyware

Cuadro 64

Nivel de conocimiento de spyware	Frecuencia	Distrib. Porcentual
Sí lo conoce	570	94.7%
No lo conoce	23	3.8%
Lo ha escuchado pero no lo	9	1.5%

conoce		
Total	602	100%

Confidencial 1

La tabla expresa en cantidad el número de organizaciones

Conocimiento de adware

Cuadro 65

Nivel de conocimiento de adware	Frecuencia	Distrib. Porcentual
Sí lo conoce	535	88.9%
No lo conoce	50	8.3%
Lo ha escuchado pero no lo conoce	17	2.8%
Total	602	100%

Confidencial 1

La tabla expresa en cantidad el número de organizaciones

Conocimiento de phishing

Cuadro 66

Nivel de conocimiento de phishing	Frecuencia	Distrib. Porcentual
Sí lo conoce	315	52.3%
No lo conoce	250	41.5%
Lo ha escuchado pero no lo conoce	37	6.1%
Total	602	100%

Confidencial 1

Conocimiento de pharming

Cuadro 67

Nivel de conocimiento de pharming	Frecuencia	Distrib. Porcentual

Sí lo conoce	225	37.4%
No lo conoce	334	55.5%
Lo ha escuchado pero no lo conoce	43	7.1%
Total	602	100%

Confidencial 1

La tabla expresa en cantidad el número de organizaciones

Conocimiento sobre troyanos

Cuadro 68

Nivel de conocimiento de troyanos	Frecuencia	Distrib. Porcentual
Sí lo conoce	580	96.3%
No lo conoce	17	2.8%
Lo ha escuchado pero no lo conoce	5	0.8%
Total	602	100%

Confidencial 1

La tabla expresa en cantidad el número de organizaciones

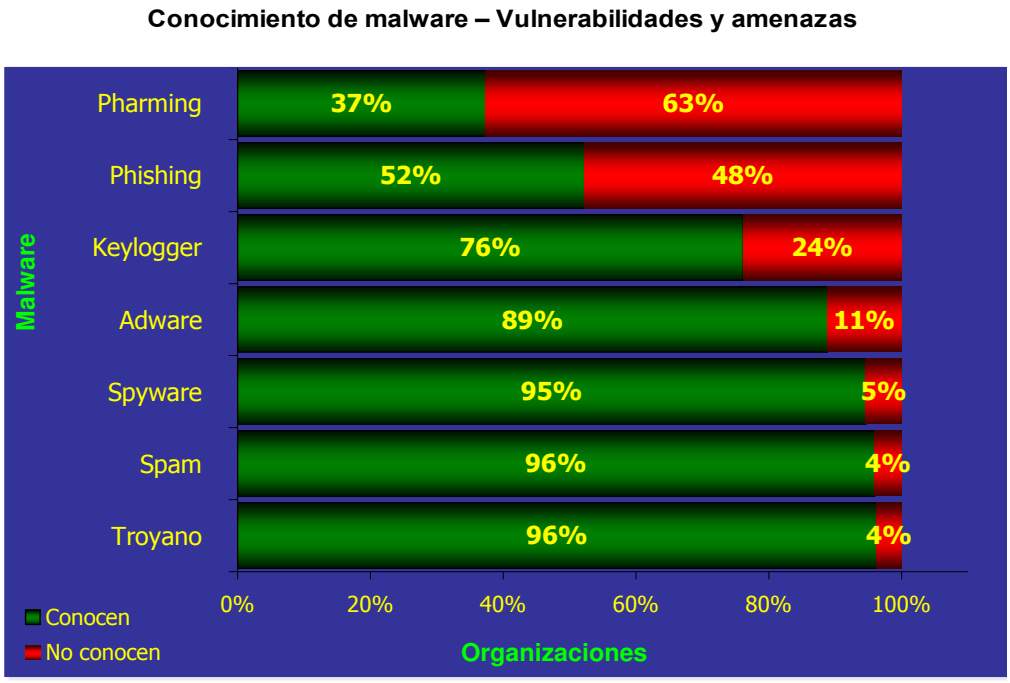
Conocimiento de keyloggers

Cuadro 69

Nivel de conocimiento de keyloggers	Frecuencia	Distrib. Porcentual
Sí lo conoce	459	76.2%
No lo conoce	124	20.6%
Lo ha escuchado pero no lo conoce	19	3.2%
Total	602	100%

Confidencial	1

La tabla expresa en cantidad el número de organizaciones



Organizaciones que sufrieron ataques de virus

Cuadro 70

Ataques de virus en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	336	55.9%
No sufrió	246	40.9%
No sabe	19	3.2%
Total	601	100%

Confidencial	2

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de gusanos

Cuadro 71

Ataques de gusanos en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	269	44.8%

No sufrió	313	52.1%
No sabe	19	3.2%
Total	601	100%

Confidencial 2

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de troyanos

Cuadro 72

Ataques de troyanos en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	265	44.1%
No sufrió	317	52.7%
No sabe	19	3.2%
Total	601	100%

Confidencial 2

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de phishing

Cuadro 73

Ataques de phishing en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	45	7.5%
No sufrió	536	89.2%
No sabe	20	3.3%
Total	601	100%

Confidencial 2

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de pharming

Cuadro 74

Ataques de pharming en el 2005	Frecuencia	Distrib. Porcentual

Sí sufrió	20	3.3%
No sufrió	561	93.3%
No sabe	20	3.3%
Total	601	100%

Confidencial 2

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de keyloggers

Cuadro 75

Ataques de keyloggers en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	36	6.0%
No sufrió	545	90.7%
No sabe	20	3.3%
Total	601	100%
Confidencial	2	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de decodificación de protocolos de red

Cuadro 76

Ataques de decodificación de protocolos de red en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	30	5.0%
No sufrió	551	91.7%
No sabe	20	3.3%
Total	601	100%
Confidencial	2	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de acceso no autorizado

Cuadro 77

Ataques de intentos de acceso no autorizados en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	141	23.5%
No sufrió	439	73.2%
No sabe	20	3.3%
Total	600	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de negación de servicios dirigidos contra los servidores

Cuadro 78

Ataques de negación de servicios dirigidos contra sus servidores en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	86	14.3%
No sufrió	494	82.3%
No sabe	20	3.3%
Total	600	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron secuestro de servidores para realizar ataques de negación de servicios contra terceros

Cuadro 79

Secuestros de sus servidores para ejecutar ataques de negación de servicios contra terceros en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	29	4.8%
No sufrió	551	91.8%
No sabe	20	3.3%
Total	600	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de buffer overflow

Cuadro 80

Ataques de buffer overflow en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	31	5.2%
No sufrió	549	91.5%
No sabe	20	3.3%
Total	600	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron ataques de hackers

Cuadro 81

Ataques de hackers en el 2005	Frecuencia	Distrib. Porcentual
Sí sufrió	72	12.0%
No sufrió	509	84.8%
No sabe	19	3.2%
Total	600	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron contaminación en sus sistemas por tener instalados programas peer to peer

Cuadro 82

Contaminación a causa de tener instalados programas peer to peer	Frecuencia	Distrib. Porcentual
Sí sufrió	75	12.5%
No sufrió	526	87.5%
Total	601	100%

Confidencial	2

La tabla expresa en cantidad el número de organizaciones

Organizaciones que sufrieron contaminación en sus sistemas por tener instalados programas de mensajería instantánea

Cuadro 83

Contaminación a causa de tener instalados programas de mensajería instantánea	Frecuencia	Distrib. Porcentual
Sí sufrió	155	25.8%
No sufrió	445	74.2%
Total	600	100%
Confidencial	3	

La tabla expresa en cantidad el número de organizaciones

Marca considerada como la más segura

Cuadro 84

Marca más segura	Frecuencia	Penetración
Cisco	192	32%
IBM	116	19%
Linux	102	17%
Oracle	83	14%
HP	80	13%
Unix	79	13%
Microsoft	49	8%
Sun	30	5.0%
Otras marcas	76	Menos de 5%
Total de casos	602	
Confidencial	1	

La tabla expresa en cantidad el número de organizaciones

Base instalada de desktops en las organizaciones

Cuadro 85

Número de desktops en las organizaciones	Frecuencia	Penetración
1 - 199	417	75%
200 - 399	65	12%
400 - 599	29	5%
600 - 799	14	3%
800 - 999	7	1%
1,000 - 4,999	21	4%
5,000 - 10,000	1	0.2%
Total de casos	554	100.0%
Confidencial	49	

La tabla expresa en cantidad el número de organizaciones

Base instalada de notebooks en las organizaciones

Cuadro 86

Número de notebooks en las organizaciones	Frecuencia	Penetración
1 - 49	440	89%
50 - 99	34	7%
100 - 149	10	2%
150 - 199	4	1%
200 - 249	4	1%
250 - 300	3	1%
Total de casos	495	100.0%
No tienen	40	
Confidencial	68	

La tabla expresa en cantidad el número de organizaciones

Base instalada de servidores en las organizaciones

Cuadro 87

Número de servidores en las organizaciones	Frecuencia	Penetración
1 - 49	537	97%
50 - 99	13	2%
100 - 150	2	0%
Total de casos	552	100.0%

No tienen 1

Confidencial 50

La tabla expresa en cantidad el número de organizaciones

Número de empleados en las organizaciones

Cuadro 88

Número de empleados en las organizaciones	Frecuencia	Penetración
1 - 199	302	54%
200 - 399	99	18%
400 - 599	53	9%
600 - 799	29	5%
800 - 999	14	3%
1,000 - 4,999	58	10%
5,000 - 10,000	4	0.7%
Más de 10,000	1	0.2%
Total de casos	560	100.0%

Confidencial 43

La tabla expresa en cantidad el número de organizaciones

Organizaciones que realizan auditorias en sus sistemas de seguridad

Cuadro 89

Realización de auditorías en sus sistemas de seguridad	Frecuencia	Distrib. Porcentual
Sí realizan	383	63.6%
No realizan	219	36.4%
Total	602	100%
Confidencial	1	

La tabla expresa en cantidad el número de organizaciones

Outsourcing de seguridad en las organizaciones

Cuadro 90

Tenencia de algún servicio de seguridad tercerizado	Frecuencia	Distrib. Porcentual
Sí tercerizan algún servicio de seguridad	40	6.6%
No tercerizan algún servicio de seguridad	563	93.4%
Total	603	100%

La tabla expresa en cantidad el número de organizaciones

Salidas del SPSS 9.0 - AFCM

Autovalores de las dimensiones

Dimensión	Autovalor
1	0.1638
2	0.0988

Medidas de discriminación

Cuadro 91

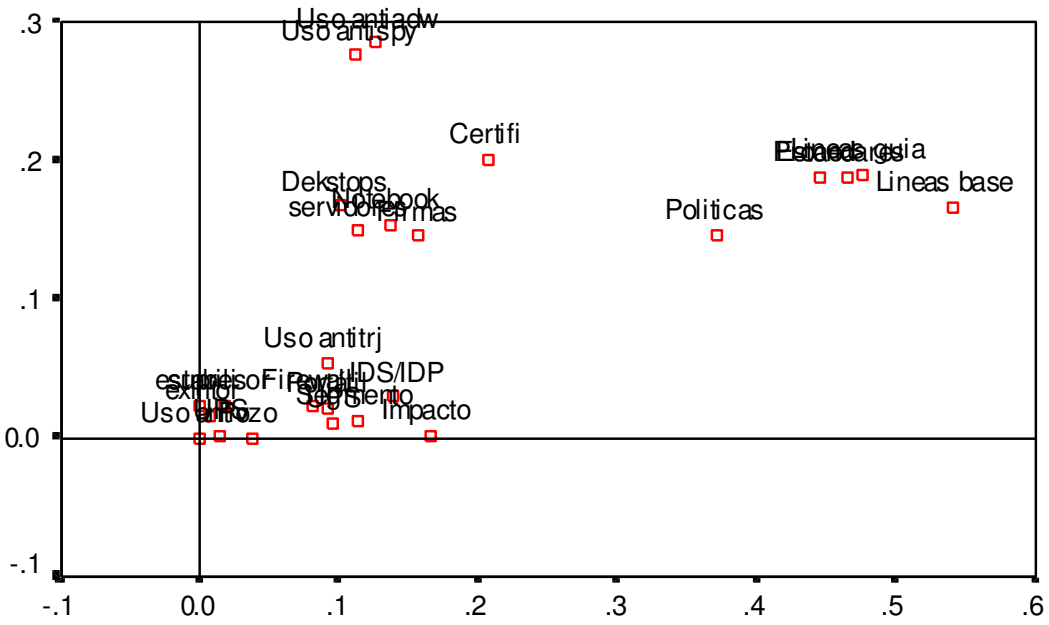
Discrimination measures per variable per dimension		
Variable	**Dimensión**	
	1	**2**
Líeas de base	0.540	0.166
Líneas de guía	0.475	0.190
Estándares	0.464	0.188
Procedimientos	0.444	0.188
Políticas	0.371	0.146
Certificado digital	0.206	0.201
Impacto	0.166	0.001
Firma digital	0.157	0.145
IDS / IDP	0.138	0.030
Notebook (BI)	0.137	0.153
Antiadware	0.126	0.285
Servidor	0.113	0.149
Antispyware	0.111	0.276
Desktop	0.101	0.167
Aire acondicionado	0.096	0.010
Antitrojan	0.091	0.055
Notebook	0.091	0.021
Firewall	0.080	0.023
Pozo a tierra	0.037	0.000
Supresor	0.017	0.022
UPS	0.014	0.001
Extintor	0.007	0.016
Antivirus	0.000	0.000
Estabilizador	0.000	0.023

Mayor valor

Gráfico de medidas de discriminación

Cuadro 92

Discrimination Measures



Mapa perceptual

Cuadro 94

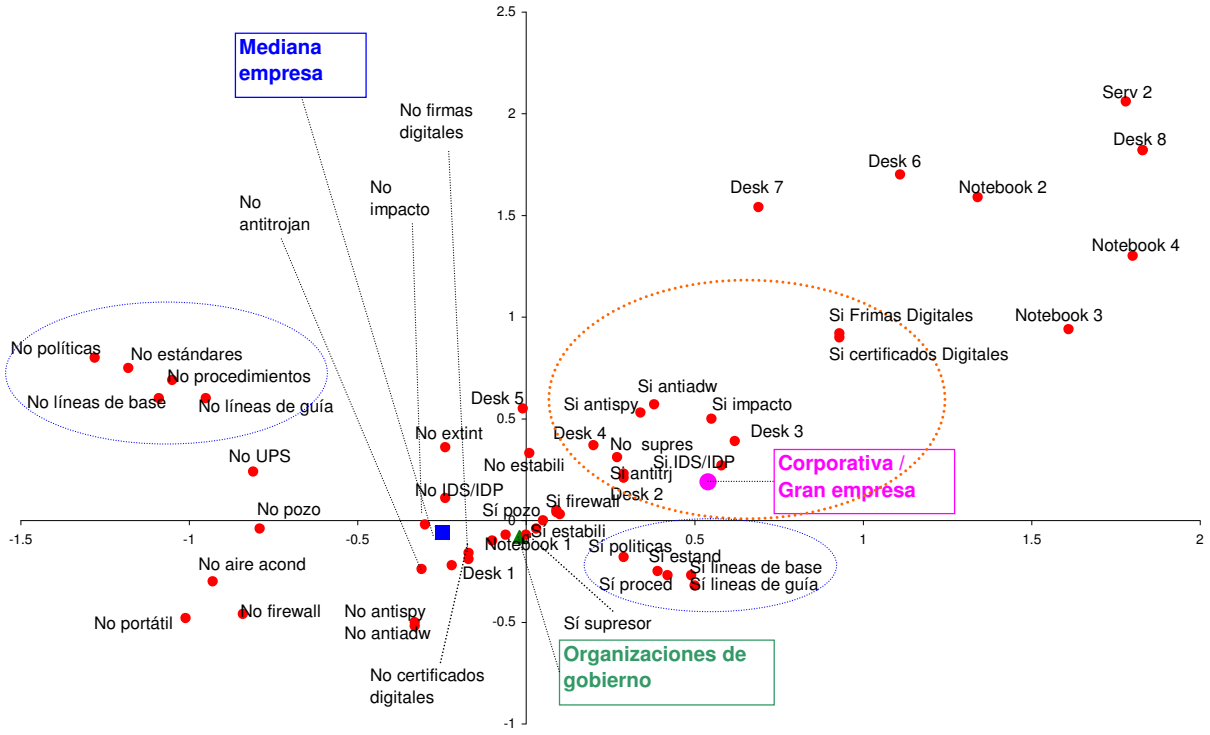
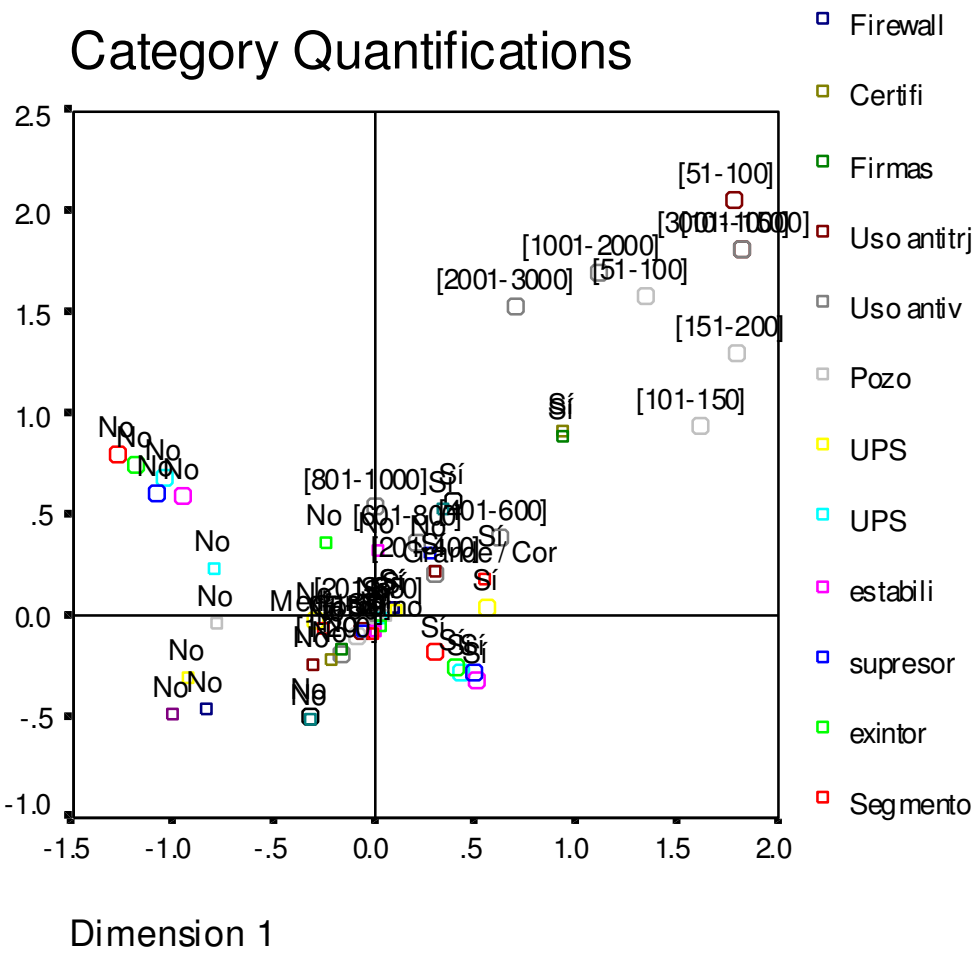


Gráfico en espacio bidimensional de las modalidades de las variables

Cuadro 95



Referencia Bibliográfica

Al Rries y Jack Trout "Las 22 leyes inmutables del marketing" Editorial McGraw-Hill Interamericana México 1994.

Celestino García Oré "Métodos estadísticos en la evaluación educacional" Concytec Perú 2002.

César Pérez "Técnicas de Análisis Multivarinate de Datos" Editorial Pearson Perú 2004.

Corina Schemelks "Manual para la presentación de anteproyectos e informes de investigación (tesis)" Editorial Harla México 1988.

Dallas E. Johnson "Métodos Multivariados aplicados al análisis de datos" Editorial Internacional Thomson Editores México 1998.

Dominio Consultores Marketing "Estudio de Seguridad Informática en en organizaciones del Perú" Estudio privado Perú 2003

Dominio Consultores en Marketing Informe del mercado peruano de cómputo Inversiones y tendencias 2005-2006" Estudio privado Perú 2005

Ficha técnica

FICHA TÉCNICA DEL ESTUDIO DE SEGURIDAD INFORMÁTICA EN ORGANIZACIONES DE PERÚ

Lima Metropolitana, Agosto 2006

El estudio logra describir el estado que presentan las organizaciones privadas y públicas en Perú en cuanto al tema de seguridad informática, empezando con una revisión del uso de políticas y procedimientos, pasando por la tenencia de hardware, software y soluciones y finalizando con la inversión que harán en este segmento del negocio IT. La investigación se basa en un cuestionario estructurado con 85 preguntas vinculadas al tema de seguridad realizado a los responsables de sistemas de las principales organizaciones del país.

Objetivos

Determinar la situación de la seguridad de sistemas en las organizaciones de Perú.

Analizar la vulnerabilidad de las empresas peruanas.

Determinar cuáles son las marcas líderes en el mercado de seguridad de sistemas.

Oportunidades de negocios

Población en estudio y muestra

Empresas localizadas en Perú pertenecientes a los segmentos corporativo-grande, mediano, y principales organizaciones de gobierno. De acuerdo con los criterios de segmentación de Dominio, pertenecen al segmento corporativo-grande todas aquellas organizaciones cuyos ingresos anuales superen los 40 millones de Dólares Americanos. Las medianas son aquellas con ingresos entre 1 y 40 millones. Las organizaciones del Estado han sido identificadas caso por caso a partir de los organigramas del sector público.

Se trabajó con muestras independientes por cada segmento con la finalidad de mantener los errores muestrales dentro de los límites adecuados para estudios de mercado. Esta estrategia de muestreo nos permitió obtener un error total de sólo 3.9%, es decir 22% inferior al error universalmente aceptado en estudios de mercado.

La estructura poblacional, el número de organizaciones por segmento, los tamaños de muestra y los errores muestrales se pueden apreciar en el siguiente cuadro:

Segmento	Población	Muestra	Error esperado
Corporaciones y Grandes empresas	309	150	5.7%
Medianas empresas	8691	320	5.4%
Principales organizaciones de gobierno	208	120	5.8%
Total	**9208**	**590**	**3.9%**

Variables en estudio

Tenencia de Políticas y procedimientos de seguridad.

Participación de mercado de las diferentes marcas tales como, supresores, UPS, estabilizadores, antivirus, antitroyanos, dispositivos de backup, firewalls, Antiadware, Antispyware entre otros

Tenencia de equipos que brindan seguridad ante incendios y fallas eléctricas.

Tenencia de soluciones que evitan o reducen las amenazas más comunes, tales como: virus, troyanos, adware, spyware, phishing, pharming, keyloggers.

Actualización de parches de sistemas operativos y aplicativos.

Realización de Backups (frecuencia, medios, y lugar de almacenamiento)

Tenencia de la solución de Disaster Recovery.

Autentificación de usuarios y de correos electrónicos.

Tenencia de niveles de acceso a archivos

Tenencia de soluciones de filtros de contenido.

Tenencia de seguridad en computadoras portátiles.

Tenencia de Firewalls.

Tenencia de IDS/IDP.

Análisis de las conductas de todos los integrantes de la organización respecto a la seguridad informática dentro de la organización.

Tendencia y tasa de cambio de la inversión en seguridad en los presupuestos de TI.

Vulnerabilidad ante diversos tipos de incidentes y amenazas de seguridad.

Incidentes experimentados durante el 2005.

Percepción acerca de la seguridad que brindan los productos Cisco, D-Link, Computer Associates, Hewlett Packard, IBM, Linux, Microsoft, Novell, Oracle, Sun, Sybase y Unix.

Outsourcing en seguridad

Cuestionario utilizado

Código de Cuestionario				

ENTREVISTADO								
CARGO								
TELEMARKETING								
EMPRESA								
FECHA								
HORA DE INICIO								
HORA DE TÉRMINO								

INCENDIOS

1. Aproximadamente, ¿Cuál es el área de su centro de cómputo?

_____ Metros cuadrados

2. Cuenta su empresa con:

	Cantidad
Extintores	
Sensores contra incendios	

SEGURIDAD ELÉCTRICA

3. Su organización utiliza:

	Sí	No
Supresores de picos?		
Estabilizadores de voltaje?		

4. ¿Utilizan UPS?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 6

5. ¿De qué marca?

_____

6. ¿Su organización cuenta con algún sistema de aire acondicionado en su centro de cómputo?

☐ Si ☐ No

Si respondió “No” pasar a la pregunta 8

7. ¿Es de precisión?

☐ Si ☐ No

8. ¿Su organización cuenta con algún pozo a tierra?

☐ Si ☐ No

ANTIVIRUS Y ANTITROYANOS

9. ¿Utiliza su compañía software antivirus?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 14

10. ¿En dónde se encuentra instalado?

A) En el/los servidor(es) (si respondió “No” pase al punto “B”)		
En el servidor de archivos		
En el servidor de correo		
En el servidor de almacenamiento		
Otros (especifique)		
Otros (especifique)		
B) En cada estación (considere a las notebooks) (*notbuks*)		

11. ¿Qué antivirus utiliza? ¿Qué tan satisfecho esta respecto al antivirus que utiliza si tuviera que calificarlo en una escala del 1 al 10, siendo 1 el menor grado de satisfacción y 10 la máxima satisfacción?

Antivirus	¿Utiliza?	Grado de satisfacción
Hacker		
Norton antivirus		

Per antivirus		
McAfee		
Sybari		
Panda		
CA		
Otros:		

12. ¿La actualización de la base de datos de virus es manual o automática?

	Manual
	Automática

13. ¿Cada cuánto tiempo se actualiza?

Cada _____(días/semanas/meses)

14. ¿Emplean software antitroyanos?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 17

15. ¿Qué antitroyano utilizan?

_____

16. ¿Qué calificación le daría al antitroyano que utiliza si tuviera que calificarlo en una escala del 1 al 10, siendo 1 el menor grado de satisfacción y 10 la máxima satisfacción?_____

17. Los parches de seguridad que realiza su empresa son manuales, automáticas o cada vez que sale una actualización en su: (marque con un aspa)

		Actualización Manual	Actualización automática	Cada vez que sale una actualización
	Sistema Operativo			

	Aplicaciones de Comunicaciones			
	Browser			
	Aplicaciones de productividad			

BACKUP

18. ¿Realizan backups *(back-aps)*/copias de respaldo en su compañía?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 23

19. ¿Cuál es la marca de la solución de backup (software) que se utiliza en su empresa?

_____

20. ¿Con qué periodicidad lo realizan? (si es diario, poner 1 en la primera opción)

Cada _____ (días/semanas/meses)

21. ¿En qué soporte realizan los backup*(backap)* : discos duros, cintas, CD, Otros (cual)?

		MARCAR CON X
	Disco duro	
	Cintas	
	CD	
	DVD:	
	Otros 1:	
	Otros 2:	

22. ¿Las copias son archivadas en la misma compañía o en algún lugar externo?

	Misma compañía
	Lugar externo
	Ambos

DISASTER RECOVERY

23. ¿Tienen implementada una solución de disaster recovery?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 27

24. ¿Quién es su proveedor?

_____

25. ¿Cuándo implementaron su solución de disaster recovery?

Semestre _____ Año _____

26. ¿Cuál de los siguientes aspectos contiene la solución de disaster recovery que tiene su empresa?

	Backup *(Bakap)* diario
	Backup *(Bakap)* remoto
	Servidores replicados
	Infraestructura alterna en caso de desastres

AUTENTICACIÓN Y CORREOS ELECTRÓNICOS

27. ¿Se usan firmas digitales en su organización?

☐ Si ☐ No

28. ¿Se utilizan certificados digitales en su organización?

☐ Si ☐ No

29. ¿El correo electrónico en su organización está encriptado o autenticado con firmas y certificados digitales? (Respuesta múltiple)

	Encriptado
	Autenticado con firma
	Autenticado con certificado
	Ninguna de las anteriores

30. ¿Se almacenan y monitorean los correos electrónicos de los usuarios?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 33

31. ¿Por cuánto tiempo se almacena esta información? _____

32. ¿Está respaldada?

☐ Si ☐ No

FILTROS DE CONTENIDO

33. ¿Se emplean filtros de contenido en su organización para monitorear el tráfico de Internet de los usuarios?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 36

34. ¿Qué tipo de contenidos filtran?

_____

_____

35. ¿Quién es su proveedor o marca de filtros de contenido que utiliza?

_____

AUTENTICACIÓN DE LOS USUARIOS PARA ACCEDER A LA RED

36. ¿Cómo se autentifica la identidad de los usuarios para el acceso a la red?

	Passwords creados por los mismos usuarios.
	Passwords creados por el departamento de Sistemas.
	Tarjetas inteligentes
	Biometría
	Ninguna de la anteriores (Pasar a la preg. 41)

37. Dichos passwords están compuestos por: (Leer las opciones) (Respuesta múltiple)

	Letras
	Números
	Símbolos o caracteres especiales

38. ¿Cuántos caracteres como mínimo acostumbra a usar para un password?

_____ Caracteres

39. ¿El área de sistemas guarda copias de todos los passwords de los usuarios en un lugar seguro?

☐ Si ☐ No

40. ¿Cada cuánto tiempo se cambian los passwords?

Días	
Semanas	
Meses	
Trimestre	
Semestre	
Año	
Otro:_____ __	

41. ¿Tiene su organización algún servidor de archivos?

☐ Si ☐ No

Si respondió “No” entonces pasar a la preg. 43

42. ¿Este(os) servidor(es) tiene algún sistema que otorgue niveles de acceso a los archivos?

☐ Si ☐ No

SEGURIDAD MÓVIL

43. ¿Existen computadoras portátiles en su organización?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 45

44. Dígame, ¿Cuál de las siguientes medidas de seguridad se emplean para garantizar la inviolabilidad de sus computadoras portátiles? (Leer las opciones)

	Algún tipo de candado físico
	Antivirus
	Passwords
	Tarjeta Inteligente
	Biometría
	Encriptación de archivos
	Software de monitoreo de ubicación
	Otro:

SEGURIDAD DE LA RED

45. ¿Emplean Firewalls *(fairwols)* para asegurar la red de su compañía?

☐ Si ☐ No

Si respondió que NO pasar a la preg. 50

46. ¿Son firewalls de hardware o de software?

	Hardware
	Software

47. De los Firewalls *(fairwols)* que tiene su organización. ¿Dónde se encuentran instalados?

	Servidores
	Estaciones
	Ambos

48. ¿Qué marca de Firewalls *(fairwols)* utilizan?

_____

49. Su Firewall (fairwols) monitorea (Leer las opciones)

	Entrada de datos
	Salida de datos
	Ambos

50. ¿Emplean algún software anti-spam? ¿Qué marca?

☐ Si ☐ No

¿Tiene?

Marca _____

Si respondió que NO pasar a la preg. 52

51. ¿Dónde se encuentra instalado?

	Servidores
	Estaciones
	Ambos

52. ¿Usa su organización IDS/IDP?

☐ Si ☐ No

53. ¿Emplean algún software anti-spyware (spaywer) , anti-adware(adwer)? ¿Qué marca?

Anti-spyware	☐	Si	☐	No
Anti-adware	☐	Si	☐	No

Marca _____Anti-spyware

Marca _____Anti-adware

54. Su browser permite la ejecución automática de contenidos activos (ActiveX)

Sí		No		No sabe	

55. ¿Cuenta su organización con una red inalámbrica?

☐ Si ☐ No

Si respondió “No” entonces pasar a la preg.57

56. ¿Ésta red inalámbrica se encuentra encriptada?

☐ Si ☐ No

57. ¿Encripta su messenger?

☐ Si ☐ No

POLÍTICAS Y PROCEDIMIENTOS

Ahora le vamos a leer una serie de conceptos, y al finalizar cada concepto quisiéramos que nos responda una pregunta.

58. Una “política de seguridad” es un documento estratégico que define el alcance de la seguridad requerida por una organización en términos de metas, misión, objetivos y propósito. Es un documento de largo plazo y demuestra el compromiso con la seguridad de la alta gerencia. Dígame por favor, ¿existen “políticas de seguridad” como las descritas en su empresa”?

☐ Si ☐ No

59. Los “estándares” definen los requerimientos compulsivos para la seguridad de una organización, el tipo de tecnología a emplear y el modo de implementación. Dígame por favor, ¿existen “estándares de seguridad” como los descritos en su empresa”?

☐ Si ☐ No

60. Las “líneas de base” salen directamente de los estándares y son un grupo específico de requerimientos de seguridad que todos los sistemas de la organización deben cumplir o exceder. Dígame por favor, ¿existen “líneas de base de seguridad” como las descritas en su empresa”?

☐ Si ☐ No

61. Las “líneas de guía” son manuales operativos que definen el modo en que deben implementarse los estándares y líneas de base. Reglamentan las condiciones para las alteraciones específicas de las líneas de base, prescriben metodologías y sugieren soluciones específicas para implementar la seguridad. Dígame por favor, ¿existen “líneas de guía de seguridad” como las descritas en su empresa”?

☐ Si ☐ No

62. Los “procedimientos” son documentos detallados que explican paso a paso cómo implantar los mecanismos de seguridad definidos en los

documentos superiores. Son específicos a una plataforma, sistema operativo, software o mecanismo de seguridad. Dígame por favor, ¿existen "procedimientos de seguridad" como las descritas en su empresa"?

☐ Si ☐ No

63. En lo que respecta a la seguridad informática (lógica y física). ¿Existen responsables? ¿A quien reportan?

Seguridad	Cargo del responsable	A quien reporta
Física		
Lógica		

CONDUCTAS Y CARACTERÍSTICAS

64. A fines del año 2005 la seguridad en su compañía era: (Leer las opciones) (Respuesta única)

	Dramáticamente más efectiva
	Algo más efectiva
	Más o menos igual
	Algo menos efectiva
	Dramáticamente menos efectiva

65. Califique el nivel de compromiso en la seguridad de la información de: (La escala a utilizar será del 1 al 10 donde el valor 1 corresponde a "Nada comprometido" y el 10 "Totalmente comprometido")

Áreas	Calificativo
Alta dirección	

Personal usuario	
Personal de Sistemas o Informática	

66. ¿Cómo se compara su presupuesto de seguridad con el que tenía antes del año 2005, usted diría que se incremento se mantuvo o redujo? ¿En que porcentaje?

		Porcentaje
	Incremento	
	Mantuvo	
	Redujo	

67. ¿Qué porcentaje del presupuesto total de sistemas/IT representa la parte de seguridad?

_____ %

68. ¿Quién tiene la autoridad final en su organización para decidir las inversiones en seguridad de sistemas?

_____

_____

69. Ha realizado su organización alguna medición del impacto (medido en US$) de un ataque que afecte el sistema de seguridad informática de su empresa?

☐ Si ☐ No

70. Utilizando una escala del 1 al 5, en donde 5 significa que es muy vulnerable y 1 significa que es nada vulnerable, como calificaría la seguridad de su empresa respecto a los siguientes temas: (Leer las opciones) (Respuesta múltiple)

		Escala
	Seguridad física o de planta ante terremotos	
	Seguridad física o de planta ante incendios	
	Seguridad física o de planta ante asaltos o robos	
	Detección de intrusos en la red	
	Prevención de intrusos en la red	

	Passwords	
	Encriptación de documentos	
	Prevención de virus	
	Protección de datos	
	Protección ante robos de computadoras	
	Seguridad del web site *(sait)*	
	Prevención de brechas internas de seguridad	
	Plan de disaster recovery	
	Revisión de antecedentes de los empleados	
	Autentificación (es un usuario quien dice ser)	

71. ¿Cree que su empresa necesita incrementar, mantener igual o disminuir su inversión en seguridad de sistemas en el 2006? ¿En que porcentaje?

		Porcentaje
	Incrementar	
	Mantener	
	Disminuir	

72. ¿Tiene conocimiento usted sobre los temas que le mencionaré a continuación? (el haber escuchado sobre el tema no significa que conozca de que se trata, es decir considere la respuesta “si lo conoce” si es que además de haber escuchado sobre el tema sabe de que se trata)

	Sí lo conoce	No lo conoce	Lo ha escuchado pero no lo conoce
Spam			
Spyware (spaiwer)			
Adware *(adwer)*			
Phishing *(fishing)*			

Pharming(farming)			
Troyano			
Keyloggers			

73. ¿Experimentó alguno de estos problemas en el 2005? (Leer las opciones) (Respuesta múltiple)

	Virus		
	Gusanos		
	Troyanos		
	Phishing		
	Pharming		
	Keyloggers		
	Decodificación de protocolos de red		
	Intentos de acceso no autorizados		
	Ataques de negación de servicios (Denial of Service) dirigidos contra sus servidores		
	Secuestro de sus servidores para ejecutar ataques de negación de servicios contra terceros		
	Ataques de buffer overflow (*bafer ouverflou*)		
	Ataques de hackers		

74. ¿Ha sufrido algún ataque o problema a causa de tener instalados programas peer-to-peer(“pir– tu- pir”)?

☐ Si ☐ No

75. ¿Ha sufrido alguna contaminación por programas de mensajería instantánea?

☐ Si ☐ No

76. Nuevamente, utilizando la escala del 5 al 1, dónde 5 representa absolutamente seguro y 1 absolutamente inseguro. ¿cuál es su

percepción acerca de la seguridad de los productos de las siguientes marcas?

Marca		Calificación
	Microsoft(“Maicrosoft”)	
	Oracle(“oracol”)	
	Sun(“San”)	
	Cisco	
	IBM	
	Unix (“yunix”)	
	Linux	
	Sybase (“say beis”)	
	Computer Associates (“compiuter asosieits”)	
	Novell	
	HP	
	D-Link	

77. Bajo un criterio muy general, independiente del producto, ¿Qué marca para usted es la más segura?

78. ¿Cuántas computadoras existen en su empresa?

Desktops	
Notebooks (“Notbuks”)	
Servidores	

79. ¿Aproximadamente, cuántas personas trabajan en su compañía?

Número de empleados	

80. Dígame dentro de cuál de los siguientes rangos se puede clasificar los ingresos de su empresa durante el 2005

	Menor a 200,000 dólares anuales
	Mas de 200,000 y menos de 1 millón de dólares anuales
	Mas de 1 millón y menos de 40 millones de dólares anuales
	Más de 40 millones y menos de 100 millones de dólares anuales
	Más de 100 millones de dólares
	No sabe
	Información confidencial

81. ¿Su organización realiza auditorias en su(s) sistema(s) de seguridad?

☐ Si ☐ No

Si respondió "No" entonces pasar a la preg. 83

82. ¿Con que frecuencia?_____

83. Existe algún servicio de seguridad informática en su organización que se encuentre bajo la modalidad de outsourcing?

☐ Si ☐ No

Si respondió "No" entonces Terminar la entrevista

84. ¿Cuáles?

_____

_____

_____

85. Me podría decir la dirección de su correo electrónico

_____@_____

Eso sería todo, muchas gracias por su colaboración. Buenos días (tardes)